

القسم الحادي عشر: الملحقات

ملحق (1): متطلبات ومعايير اداره المشاريع Project Management

- **المتطلبات العامة لإدارة المشروع**

يجب أن يرفق المقاول خطة وتفصيل لمنهجية إدارة المشروع مع العرض الفني بحيث تشمل نطاق المشروع بحيث تحقق المتطلبات الآتية:

- تطبيق أفضل ممارسات ومنهجيات إدارة المشاريع المعتمدة عالميا في إدارة المشروع.
- تحديد الهيكل التنظيمي المفصل لفريق عمل المشروع.
- توفير نقطة اتصال واحده للمشروع (مديرا المشروع)
- تحديد أعضاء فريق العمل الذين يعملون بالمشروع بدوام كامل في موقع المشروع والمسمى الوظيفي والمهام والمسؤوليات لكل منهم
- خطة لإدارة الاتصال (Communication Management) : ضمن المشروع.
- خطة إدارة القضايا والمشاكل الطارئة (Issue Management)
- خطة إدارة التغير Change management
- خطة إدارة المخاطر (Risk Management) : والعمليات والإجراءات المتبعة في إدارة المخاطر
- خطة إدارة التوثيق (Document Management) : والإجراءات المتبعة في إدارة التوثيق من حيث مراجعة وفحص المخرجات.
- العلاقة بمقاولي الباطن
- الإجراءات اللوجستية لشراء الأجهزة وتسليمها وعمليات الجرد
- مراقبة سير أعمال المشروع والتقارير الدورية لذلك

- **ادارة المشروع**

- تعد شروط وزارة الدفاع المفصلة في هذا الملحق جزءا من العقد.
- يعد جزءا من العقد كافة الوثائق اللازمة لتحديد نطاق العمل والتزامات المتعهد، ويشمل ذلك وثيقة طلب العروض، وعرض المتعهد، وأي مراسلات لاحقة توضح وتوثق التزامات المتعهد وأي استثناءات أو إضافات يتفق عليها في مرحلة المفاوضات للتعاقد. ويمكن الاستعاضة عن ذلك باعتماد وثيقة شاملة تفصل جميع بنود نطاق العمل وتوضح تحديدا الوثائق التي تستبعد بناء على ذلك.
- يقع تنفيذ هذا الحل والمشروع المبني عليه تحت إشراف ومتابعة الجهة المشرفة على العقد بوزارة الدفاع.
- سيتم تعيين المشرف على المشروع (Project Owner) من قبل الوزارة، والذي سيمثل الوزارة في الإشراف والمتابعة والاعتماد لمخرجات تنفيذ الحل ومراحله المختلفة، ويجب أن يعمل مدير المشروع وفريق العمل المعين من قبل المتعهد تحت إدارة وإشراف ومتابعة يومية من قبل المشرف على المشروع وفريقه بشكل يومي.
- يحق للوزارة تكليف من تراه من المختصين داخلياً أو خارجياً لمراجعة وتقييم مخرجات المشروع للتأكد من مطابقتها للشروط والموصفات وعلى المتعهد تقديم المساعدات اللازمة لتمكين هؤلاء المختصين من القيام بواجباتهم.
- يعد أي تأخير في تسليم أيٍ من المتطلبات/ المخرجات المحددة بوقت في هذه الوثيقة، سبباً لإنذار المتعهد، وقد يؤدي ذلك إلى فرض غرامة تأخير أو تنفيذه عن طريق مقاول آخر على حساب ونفقة المتعهد أو إلغاء العقد وسحب كامل المشروع مع تحمل المتعهد كامل التكاليف المترتبة على ذلك.
- يجب على المتعهد الاستفادة من الموارد المتاحة في الوزارة قدر المستطاع، سواء لإدارة أو تنفيذ المشروع، ويجب عليه توضيح ذلك تفصيلياً من ناحية الأعداد والكفاءات والخبرات المطلوبة وطريقة التفرغ المطلوب.

- **منهجية المشروع**

ينبغي على الشركات المقدمة لتنفيذ الحلول تقديم عرض تفصيلي لمنهجية تنفيذ الأنشطة الرئيسية للمشروع محل الاتفاق، والمحتوى والمدة، وطريقة تقسيم مراحل العمل والعلاقات المتبادلة فيما بينها، مع توضيح لتواريخ تسليم كل مخرج من المخرجات المتفق عليه في نطاق المشروع وفق إطار زمني تتفق مع ما يلي:

- سوف يتم اعتماد منهجية المعهد الدولي لإدارة المشاريع الاحترافية (PMI) في إدارة هذا المشروع، وذلك لإضافة عنصر داعم لنجاحه، وعليه سوف تقدم الشركة المنفذة ما يثبت قدراتها على إدارة هذا المشروع بشكل احترافي و باعتماد تلك المنهجية.
- وبناء على ما سبق فإن جميع العروض تكون وفق المنهجية المعتمدة والتي تتضمن خطط عمل المشروع والجدول الزمني للأنشطة التي سيتم إنجازها والمسؤولين عنها.
- على مقدمي العروض تقديم منهجية دقيقة لضمان تحقيق في كل مخرجات المشروع.



- على المتعهد إيضاح المنهجية المستخدمة في تنفيذ وتسليم المشروع (Project Approach) من خلال تحليل متطلبات المشروع، منهجية التطوير، ومنهجية اختبار وتشغيل الأنظمة وكما هو موضح في نطاق عمل المشروع.

- **موظفو المشروع**
  - **فريق العمل من قبل المتعهد**
    - يجب على المتعهد توفير الموارد البشرية الاستشارية والإدارية والفنية المؤهلة لتنفيذ متطلبات المشروع مع تقديم ما يثبت ذلك، ويجب أن يكون لكل مرشح الخبرة اللازمة والمطلوبة في وثيقة طلب العروض كحد أدنى، كما يجب تقديم السير الذاتية للمرشحين للحصول على الموافقة الخطية أو بالبريد الإلكتروني الرسمي من قبل المشرف على المشروع.
    - يجب أن تكون السيرة الذاتية لأي مرشح دالة على قدراته في مجال العمل المرشح له بما يكفي لإقناع صاحب القرار بقبوله.
    - للوزارة الحق بطلب تغيير أو استبعاد أي موظف خلال مدة العقد بناء على أداءه، ويجب على المتعهد توفير البديل المناسب خلال مدة أقصاها (٢٠) أيام عمل من تاريخ إبلاغه بالتغيير ودون أن يتأثر العمل بذلك، مع التزام الأول بتسيير العمل حتى يتم تسليم ما لديه والتأكد من قدرة البديل على إكمال العمل.
    - يُعَد عدم الالتزام بالمدة المحددة لترشيح وتعيين موظفي المشروع تأخيرا من قبل المتعهد وسببا للإنذار قد يؤدي إلى فرض غرامة تأخير أو إلغاء العقد وسحب المشروع. ويشمل ذلك أي تأخير ينتج عن تقديم مرشحين غير مؤهلين يرفضهم المشرف على المشروع.
    - يجب عدم تغيير أي موظف من قبل المتعهد إلا بعد موافقة الوزارة عليه، إلا إن كان ذلك لخروج/استقالة الموظف من العمل لدى المتعهد (أو المقول من الباطن)، ويجب في هذه الحالة إخطار الشركة والمشرف على المشروع فورا، على أن يستمر في العمل وفق المدة المنصوص عليها بنظام العمل السعودي وينقل ما لديه من عمل إلى بديل يوفره المتعهد بموافقة المشرف على المشروع.
    - يجب على المتعهد (المقاول) الإلتزام بتوفير فريق العمل المطلوب لتنفيذ متطلبات المشروع حسب الكفاءات الفنية والإدارية والموضحة بجول مواصفات العمالة والشروط الخاصة.
    - للوزارة الحق في التفاوض مع أيٍ من أعضاء فريق العمل الرئيس للمشروع، ونقل خدماته إليها أو إلى متعهد آخر بعد انتهاء المشروع دون أي اعتراضٍ من قبل المتعهد.
    - يجب على المتعهد تقديم جدول زمني واضح وحسب المدة المحددة في العقد لتوفير موظفي المشروع (حسب حاجة المشروع) ويخضع الجدول للموافقة الخطية أو بالبريد الإلكتروني الرسمي من قبل المشرف على المشروع.

  - **مدير المشروع (من جهة المتعهد)**
    - يجب على المتعهد تعيين مدير المشروع، وفق الشروط المتفق عليها، وذلك خلال (٢٠) أيام عمل من تاريخ استلام التعميد.
    - يجب أن يكون مدير المشروع متفرغا لإدارة المشروع بدوام كامل ولا يتم تكليفه بأي أعمال خارجية، ويعمل في مكتب يحدد له في مقر الشركة/الوزارة.
    - يجب على مدير المشروع التواجد بشكل دائم، وتنسيق أي تغيب عن العمل مع المشرف على المشروع خطياً أو بالبريد الإلكتروني الرسمي، سواء كان ذلك لعمل أو أجازه أو أي سبب آخر، مع ضرورة توفير بديل مؤهل لا يقل عنه خلال فترة غيابه.
    - يجب على مدير المشروع القيام بدوره على أكمل وجه وبالأعمال التالية على سبيل المثال لا الحصر:
      - التمثيل الكامل للمتعهد/المقاول في جميع ما يتطلب ذلك مع الوزارة ويكون مخولاً لاتخاذ القرارات نيابة عن المتعهد والمقاولين من الباطن.
      - متابعة وتوجيه فريق عمل المتعهد لتنفيذ متطلبات المشروع طوال مدة العقد.
      - إدارة ومعالجة العوائق والمخاطر، وتصعيد ما يلزم إلى المشرف على المشروع أو اللجنة التوجيهية للمشروع حسب الحاجة.
      - إعداد ورفع تقارير سير العمل والإنجاز ومؤشر الأداء الزمني للمشروع بشكل دوري. ويجب أن تشمل هذه التقارير النسبة المئوية الفعلية للمنجز والقيمة المكتسبة المحققة من المشروع (Actual % Complete & Earned Value).
      - التنسيق الكامل والغير مخل بما يواجه المشروع مع المشرف على المشروع بشكل مستمر حول سير المشروع، وأخذ الموافقات اللازمة حسب المتطلبات في هذه الوثيقة وفي العقد.
      - إدارة العلاقة مع أصحاب المصلحة من المشروع بالتنسيق مع المشرف على المشروع (Stakeholder Management).
      - إكمال المتطلبات في جميع مراحل المشروع (تعبئة نماذج، تحديث بيانات، متابعة إجراءات العمل ....) على الأنظمة الآلية المتعلقة بإدارة المشروع في الشركة/الوزارة.
      - الاجتماع دورياً مع اللجنة التوجيهية للمشروع (Steering Committee).



- **المرحلة الانتقالية**
  - يجب على المتعهد وضع خطة لإدارة انتقال أي مخرجات يجب استلامها وتشغيلها إلى أي جهة تخولها الوزارة، وضمان اكتمال الانتقال قبل نهاية مرحلة التشغيل بمدة (ستة) أشهر على الأقل.
  - يجب على المتعهد تنسيق جميع الأنشطة الانتقالية مع أصحاب العلاقة في الوزارة والحصول على موافقتهم على أي وثائق أو تعديلات تمس عملهم.
  - يتحمل المتعهد كامل المسؤولية عن ضمان سير العمل في هذه المرحلة حسب ما هو مخطط له، ولا تنتهي مسؤوليته إلا مع التوقيع النهائي لقبول المخرجات النهائية للمشروع.

- **الوثائق والمراجعات**
  - يعتمد نجاح المشروع على التوثيق الصحيح والمنهجي بالطرق المعتمدة عالمياً في جميع مراحله، بدءاً من مرحلة التعاقد، مروراً بمراحل التنفيذ المختلفة، وانتهاءً بوثائق المخرجات النهائية وتسليم المشروع.
  - ويوضح هذا الباب متطلبات التوثيق الأساسية لهذا المشروع، علماً أنه يجب أن يحصل المتعهد على موافقة المشرف على المشروع على جاهزية وصلاحية ومنهجية كافة وثائق المشروع.

- **وثيقة نطاق العمل (SOW)**
  - يجب على المتعهد العمل مع المشرف على المشروع لإعداد وثيقة نطاق العمل والتي تحدد مخرجات المشروع كاملة (Statement of Work)، بما في ذلك كل ما هو مطلوب في وثيقة طلب العروض وأي إضافات أو استثناءات أو تعديلات تم الاتفاق عليها في مرحلة التفاوض، إضافة إلى المنهجيات والإجراءات التي ستستخدم في تنفيذ المشروع.
  - تعتبر وثيقة نطاق العمل جزءاً لا يتجزأ من العقد ولا يكتفى بها عنه ولا عن باقي ملاحقه المتفق عليها، ويجب إتمامها خلال ١٠ أيام عمل من الإخطار بالفوز.

- **خطة التنفيذ المبدئية**
  - على المتعهد تحديث الجدول الزمني للمخرجات الرئيسة (لمستويين هيكليين للمخرجات المستهدفة) للمشروع يوضح مراحل تنفيذ وإدارة المشروع ضمن المدة الإجمالية المحددة.
  - للأنظمة التقنية، يجب أن توضح الخطة بداية التشغيل المبدئي (التجريبي)، وكافة مراحل التشغيل، منتهية بالقبول النهائي.
  - يجب استخدام (MS Project) إصدار ٢٠١٣ أو أحدث.

- **خطة التنفيذ التفصيلية**
  - يجب على المتعهد، إعداد خطة التنفيذ التفصيلية للمشروع (Project Execution Plan "PEP")، ويكون ذلك بالعمل مع أصحاب المصلحة الرئيسيين والمشرف على المشروع، علماً أنه يجب الحصول على موافقة المشرف على المشروع على الخطة بكامل أجزائها وتفاصيلها.
  - يجب أن تشمل الخطة جدول زمني مفصل يشمل تفاصيل الأنشطة الرئيسية، والمخرجات ومراحل التنفيذ والأنشطة الفرعية والمهام المتعلقة ومتطلبات الوقت والجداول الزمنية، والعلاقة والاعتماديات بين مراحل المشـــروع و الارتباط فيما بينها، وما إلى ذلك، وذلك بتقديم تفصـــيل هيكلي كامل للعمل بجميع مســـتوياته إلى آخر مســـتوى/وحدة يمكن تقســـيمها والعمل عليه/عليها باستخدام طريقة (Work Breakdown Structure "WBS") وهذه الجزئية (وثيقة منفصلة ملحقة بوثيقة نطاق العمل) يمكن تأخير تقديمها إلى ما بعد إقرار وثيقة SOW بمدة لا تتجاوز عن ١٠ أيام عمل.
  - يجب أن يشمل الجدول الزمني تحديد بداية عمل التنفيذ وتوضيح المسار الحرج الجزئي لمراحله المختلفة وكامل للمشروع.
  - يجب أن تشمل تفاصيل الأنشطة المختلفة وأدوار ومسؤوليات موظفي المتعهد لكل منها حسب ما تم تفصيله في (WBS) المذكور آنفاً.
  - يجب أن تظهر الخطة بوضوح أي اعتماديات وافتراضات على الشركة أو الوزارة ومبررات ذلك (إن وجد).
  - يجب إدارة الخطة التنفيذية التفصيلية وتمثيلها باستخدام (MS Project) إصدار ٢٠١٣ أو أحدث.

- **ضمان الجودة**

يتحمل المورد مســـؤولية جودة المخرجات التقنية. يجب أن يمنح المورد وزارة الدفاع الحق في الوصـــول إلى جميع بيئات الاستضافة التطويرية. تحتفظ وزارة الدفاع لنفسها بالحق في فحص وإجراء أي اختبارات و / أو قياسات ضرورية على كل أو أي جزء من الحل في أي مرحلة. تحتفظ وزارة الدفاع بالحق في رفض كل أو أي من المكونات التي لا تتوافق مع المواصـــفات المتفق عليها.

يجب أن يتضـــمن العرض الفني للمقاول على خطة ومنهجيه لإدارة الجودة واختبار الأنظمة والخدمات المقدمة بما يضـــمن أعلى معايير الجودة. ويجب ان تحقق المنهجية المقترحة الشروط التالية كحد أدنى وليس على سبيل الحصر:

- تقديم منهجية تفصيلية لعملية اختبار الأنظمة والمنتجات تتوافق مع احتياجات الوزارة وتغطي متطلبات الأمن السيبراني في الوزارة وضوابط الهيئة الوطنية للأمن السيبراني

- تغطية الاختبارات اللازمة من قبل المورد قبل تسليم النظام لاختبارات قبول الوزارة (UAT) على سبيل المثال لا الحصر اختبارات Unit Test, Product Test, Interface Test, Installation Test, Integration Test, Full Functional End to End test) وكذا والاختبارات الأمنية اللازمة
  تقديم المستندات الداعمة للاختبارات المنفذة من قبل المقاول والتي سيتم مراجعتها والموافقة عليها من قبل الوزارة (Test Scope, Test Plan, Test Cases, Identified Defects)
- سيتم عمل اختبارات قبول النظام من قبل الوزارة على مرحلتين:
  - المرحلة الأولى: من قبل فريق الجودة والاختبار من المورد.
  - المرحلة الثانية: من قبل فريق إدارة الأعمال وملاك النظام.
  - يتم البدء بالمرحلة الثانية بعد اجتياز المرحلة الأولى بنجاح وتحقيق معايير اجتياز الاختبارات.
- يجب على المورد توفير المستندات والوثائق الخاصة بالأنظمة محل التطوير لفريق الوزارة للجودة والاختبار لتمكينه من تجهيز وإعداد اختبارات الجودة التي سينفذها في مرحلة قبول المنتج.
  - يجب على المقاول تجهيز بيئة اختبارية مطابقه للبيئة الفعلية وتجهيز أي بيانات لازمه لتنفيذ الاختبار.
  - يجب على المقاول تجهيز قائمه اختبار للجاهزية التشغيلية والأمنية بحيث تستخدم عند نقل النظام الى البيئة الإنتاجية للتحقق من سلامة النقل وجاهزية النظام لتشغيل.
  - يجب على المقاول إصلاح ومعالجة المشاكل (Defects) الظاهرة في نتائج الاختبارات.

ملحق (٢): المتطلبات الفنية للمشروع

Requirement	Compliance (Yes/No/Partial)	Additional Notes/Justifications (Mandatory if “Partial” is chosen)
Deployment and Product Integration		
The solution should support all the major Firewalls such as Cisco ASA & FTD, PaloAlto, Fortinet, etc…		
Solution should support integration with NSX-T, support should include policy visibility, risk and compliance report generation, change monitoring if added later into the solution		
Solution should support integration with F5 LTM and AFM, support should include policy visibility, risk and compliance report generation, change monitoring and Baseline reports.		
Solution should have Issues Center inbuilt in the GUI which should have focused picture of all current product issues for enhanced & timely troubleshooting		
Solution should support L3 Devices from Routing/Topology Map perspective such as Cisco IOS/Nexus, HP and Juniper if added later into Firewall Analyzer solution		
Risk Management		
Solution should be capable of running Risk Identification from Non-Secured to Secured Zones enforcing strong network segmentation		
Solution should allow whitelisting the Risky Traffic		
Solution should support defining an expiry date for Whitelisted traffic, for example “a given Risky Rule should be whitelisted for a period of 1 month”		
Solution should support aggregating all devices to a single logical unit/group to generate a group-based report using a single risk profile		

Audit - Ready Compliance		
Solution should allow GUI based customization of Baseline compliance profiles for the Firewalls and generate the report highlighting violations if any		
Solution should provide below auto-completed compliance/Audit reports for Individual and for group of firewalls –		
ISO 27001		
NERC		
Basel II		
SOX & JSOX		
PCI DSS		
NIST		
Configuration Change Compliance		
Solution should generate a baseline configuration compliance report that compares device configurations to predefined baselines and reports exceptions for Cisco ASA/FTD, PaloAlto, F5(LTM & AFM) Juniper (SRX & Netscreen), Checkpoint & Fortinet Firewalls		
Solution should alert for all the policy / Configuration changes made on the respective Firewalls		
Solution should be capable of generating Reports and charts clearly displaying changes in Baseline Compliance with every single requirement in the Baseline Configuration Profile		
Firewall Policy Optimization		
Solution should provide info on –		
Redundant special case rules		
Unused rule items		
Disabled rules		
Time-inactive rules		
Duplicate object and services		
Rules without logging		
Rules with non-compliant comments		
Rules with empty comments		
Rules about to expire		
Solution should report on how to tighten overly permissive rules (IPT) on firewalls E.g., Rules having ANY source, ANY destination, ANY service should break down to get an actual traffic passing through that rule		
Solution should provide information on rule Reordering with Actionable modification recommendation based on RMPP		
Suggest the most valuable Rule Reordering with an expected improvement on the utilization of the device based on RMPP		
Solution should provide report on Object usage within the Rule for Cleanup		
Solution should provide report on both unattached and unused objects		
Solution should suggest consolidation of Rules for optimizing the rules set for better manageability, audit, and performance		
Access Control		

Solution should support Role based operation, allows groups of firewalls, users, and permissions, including granular permissions for report viewing and device actions		
Solution should support mapping user roles to Active Directory/ LDAP groups		
Solution should have a client Web interface i.e., no client software installation be installed to access the GUI		
Operations Management		
Solution should support running a root cause analysis / query in multiple-firewall multiple-vendor environment		
Solution's Traffic Simulation query should support application name or service-based query to find out the relevant blocked and allowed policies on the Firewalls		
Solution should have GUI to customize Hardening/Baseline Profiles for all the supported devices		
Change Automation		
Solution shall provide native multiple Change Request Submission Methods, including:		
Native User Interface (Web Portal)		
Native XLS/CSV Parsing		
Solution shall provide native capability to automatically Determine Devices Requiring Policy Change		
Solution shall provide native capability to automatically Proactively Assess Risk of Proposed Changes		
Solution shall provide native capability to automatically create Plan Vendor Specific Implementation Plans		
Solution shall provide native capability to automatically Implement or Stage New Policies/NSGs On Cisco ASA, PaloAlto via Panorama, Fortinet via Fortimanager, Checkpoint via Smartcentre server, Juniper SRX & Netscreen, Cisco ACI and VMWware NSX-T		
Solution shall provide native capability to automatically Validate the Accuracy of Changes Post-Implementation		
Solution shall provide native capability to automatically Map Historical Change Requests To Security Policies on devices		
Solution shall provide native capability to expose Rule Removal automation		
Solution shall provide native Traffic Request Recertification, focusing on recertifying the traffic & business need of historical requests		
Solution shall provide native Object Management & Automation, focusing on manipulating object contents based on direct requests (Add/Modify/Delete)		
To assess an impact on critical Application during Firewall/Server migration/upgradation/decommissioning the proposed NSPM solution should allow conducting an Impact Analysis from Business Application perse where it should list down all the applications which will be		



impacted during Firewall/Server migration/upgradation/decommissioning project		
Solution shall automatically map Business Applications to Change Requests, which originate from changes to the application flows		
General Features		
In its normal operation mode (without faults or customizations), the proposed solution should allow instant and scheduled simulations on the following basis: a. Once b. Daily (Every 1 to 7 days on a specific time) c. Weekly (Every 1 to 4 weeks on a specific day and time) d. Monthly (Every 1 to 4 months on a specific date and time) e. i.e., Every two months repeating on 7 and 23 at 02:00 PM, starting on Thursday, September 7th, 2024.		
The proposed solution should be able to run parallel simulations with multiple agents.		
The proposed solution should let the users update the agents with a single click on the management.		
The proposed solution should be a software-only solution to automatically test the effectiveness of the security controls used by the organization via the below-stated terms.		
The proposed solution should provide adequate information for each attack simulation to identify each attack in any of the security devices under test.		
The proposed solution should provide access to MITRE ATT&CK framework coverage in the web interface for each simulation.		
The proposed solution should be able to show success/failure scenarios in the MITRE ATT&CK framework on a tactical and technical basis in the web interface.		
The proposed solution should provide zero false-positive results which means any attack reported as not-prevented by installed security controls can be proved as such. Upon request, the supplier will perform the necessary work to prove truthfulness of the not prevented attack status.		
The proposed solution should be able to test the security efficacy of client, network, virtualization, and cloud security systems of the institution by performing attack simulations among software components that can be installed in a distributed structure.		
The proposed solution should be able to assess the security level provided by a group of endpoints and/or network security technologies that work in isolation or are integrated with other security systems, independent of the underlying vendor and technology.		
The proposed solution should simulate attacks, report findings, and be able to propose mitigations		



continuously and a near-real-time basis for each attack scenario.		
The proposed solution's components should run attack simulations among its components and should not initiate connections to any production applications and endpoint systems to provide a risk-free assessment unless configured for lateral movement.		
Endpoint security control assessments should be constrained in the designated computer system(s) and this assessment process should not interact with other systems unless configured for lateral movement.		
The proposed solution should be able to integrate with Palo Alto Cortex XSOAR to create custom playbooks to develop specific scenarios to improve analysts' effectiveness.		
The proposed solution should be able to integrate with Palo Alto Cortex XSOAR for the following purposes: a. Create custom playbooks to develop specific scenarios to improve analysts' effectiveness. b. After a new threat is added to the Threat Library, use Cortex XSOAR to schedule an attack simulation. c. Pull mitigation suggestions directly from the Platform's mitigation library into Cortex XSOAR and use them in the playbooks to accelerate automation. See which threats were blocked or missed and remediate gaps automatically		
API and Integrations		
The proposed solution should have the following features available for GET functions via API: a. Agent List and Details b. Integrations and Integration Details c. Mitigation Device List and Signature List d. Simulation List and Details e. Detailed Simulation Results f. MITRE Mapping for Simulation Results g. Threat Template Operations Threat List and Detailed Information		
The proposed solution should have the following features available for POST/PUT/DELETE functions via API: a. Agent Token Information b. Create/Start/Stop/Update/Delete Simulation Create Threat Templates		

The proposed solution should support integration and communicate with other solutions based on an "Application Control Interface" (API) access or the Syslog protocol, for purposes such as: a. Customized reports b. Customized dashboards c. Integration with third party solutions like SOAR, SIEM or other platforms d. Creating Dynamic & Static Templates e. Creating Simulations & Re-run Simulations f. Export Mitigations Export Threat Lists		
The proposed solution should be able to integrate with ticketing and communication systems such as: ServiceNow		
Threat Library & Threat Templates		
The Threat Library included in the proposed solution shall receive updates on a near daily basis.		
The proposed solution should provide emerging threats without any extra licenses. If needed, extra licenses should be included in the offer.		
The proposed solution should provide ready to use static threat templates for Emerging and Suggested Threats that can also be modified by the user for customized needs.		
The proposed solution should provide ready to use dynamic threat templates for Security Posture Management such as Readiness Against Ransomwares, Readiness Against APT Groups, and Security Control Rationalization such as Network Security (IPS/IDS & NGFW Testing, WAF Testing, DLP Testing, Web Security Gateway Testing), Endpoint Security Testing, and Email Security Testing.		
The proposed solution should provide the aforementioned dynamic templates to be customized by the user.		
The proposed solution should provide the custom creation of dynamic templates with filters such as; Threat Name, Tags, Attack Category, Threat Actors, Unified Killchain, MITRE ATT&CK Tactics, Affected OS, Severity, and Release Date.		
The proposed solution should be able to automatically add newly added attacks to the dynamic templates without user intervention.		
The proposed solution should allow users to simulate all available attack module actions for posture visibility.		
The proposed solution should use real-world malicious attack payloads for File Download, Email, and Web Application Attacks while testing network security controls.		
Threats contained in the threat database should be referenced according to the following set of information, including but not limited to:		

a. Unique identification number of the threat (unique ID) b. Release date of the threat c. A text-based description of the threat SSO d. The severity of the threat is according to the following scale: Low, Medium, High. e. Affected Platforms, f. Targeted Sector, g. Targeted Region h. Attacker's Objectives, i. Actions, j. Payloads, Executed Process Command Lines or Hash Values based on Attack Type, k. References in publicly known databases: virustotal l. References in the following industry-recognized threat scoring and enumeration systems: CVE, CWE, CVSS, OWASP. Operating systems affected by the threat		
The proposed solution shall allow assessment results of "blocked" and "not blocked" threats to be exported via CSV format.		
Network Infiltration (File Download) Attack Module		
The proposed solution's attack database should include at least 1800 (one thousand and eight hundred) network infiltration (file download) threats in the threat library.		
The proposed solution should support HTTP & HTTPS protocols for testing network security controls. All applicable Network Infiltration (file download) attacks should run over these protocols.		
The proposed solution should be able to support browser agents for quick IPS/IDS/Web Gateway testing over HTTPS.		
Email Infiltration Attack Module		
The proposed solution should perform SMTP tests from the internet to the corporate domain.		
The proposed solution should perform URL attacks by using the SMTP protocol from the internet to the corporate (email) domain.		
The proposed solution should perform Attachment attacks by using the SMTP protocol from the internet to the corporate (email) domain.		
The proposed solution should support an agentless Email Simulator for email attack tests.		
The proposed solution's attack database should include at least 1400 (one thousand four hundred) unique email threats in the threat library.		
Web Application Attack Module		
The proposed solution should perform Web Application Attacks over both HTTP and HTTPS.		
The proposed solution should allow users to change HTTP and HTTPS default ports.		
The proposed solution's attack database should include at least 204 (two hundred and four) unique web application attack signatures in the threat library.		

The proposed solution should use actual threat payload for security control assessment rather than using "PCAP playing" for web application attacks.		
Endpoint Attack for Windows Module		
The proposed solution should imitate malicious methods used by APT's (Advanced Persistent Threats) while testing Windows endpoint security controls, without infecting the underlying operating system.		
The proposed solution should cover at least 120 MITRE ATT&CK Enterprise framework techniques for Windows operating systems.		
The proposed solution's attack database should include at least 110 (one hundred and ten) unique windows endpoint scenarios in the threat library.		
Endpoint Attack for Linux Module		
The proposed solution should imitate malicious methods used by APT's (Advanced Persistent Threats) while testing MacOS endpoint security controls, without infecting the underlying operating system.		
The proposed solution's attack database should include MacOS endpoint scenarios in the threat library		
Data Exfiltration Module		
The proposed solution should be able to validate endpoint and network DLP solutions.		
The proposed solution's attack database should include at least 19 (nineteen) unique data exfiltration samples in the threat library.		
The proposed solution should cover exfiltration techniques at least over HTTP, HTTPS, and TCP protocols.		
The proposed solution should cover at least XOR Encryption and Base64 Encoding obfuscation methods		
URL Filtering Module		
The proposed solution should be able to validate solutions like Proxy and URL filtering.		
The proposed solution's attack database should include at least 20 (twenty) URL categories with at least 7000 URLs.		
The proposed solution should be able to enable users to customize the result decision to prevent false positive result decisions.		
Custom Attack Module		
The proposed solution should allow users to create custom Windows Endpoint Scenario attacks using MITRE ATT&CK framework action library with at least 1000(one thousand) Endpoint Scenario Actions available.		
The proposed solution should allow users to create custom Network Infiltration (File Download) attacks using existing threat library with at least 8000(eight thousand) malicious files available.		
The proposed solution should allow users to create custom Web Application attacks using the existing threat library with at least 2000(two thousand) malicious payloads available.		

The proposed solution should allow users to upload their custom Web Application payloads to the Threat Library.		
The proposed solution should allow users to create custom Email attacks using the existing threat library with at least 7400(seven thousand and four hundred) malicious files available.		
The proposed solution should allow users to upload their custom Malicious Codes or Vulnerability Exploits to the Threat Library.		
The proposed solution should allow users to create custom Data Exfiltration samples using the existing threat library with at least 200 (two hundred) sample files available.		
The proposed solution should allow users to upload their custom attacks for web application attack, email attack, network infiltration attacks and data exfiltration attack modules.		
The proposed solution should allow users to add Play and Rewind processes with the following information to be added: a. Path and Argument b. Ability to Add a Remote File c. Ability to Use a Local File d. Define Result Logic e. Metadata Information Action Details		
Mitigation		
The proposed solution should display the utilization and effectiveness level of a vendor technology, expressed as a percentage, number of blocked and not blocked threats per simulation.		
The proposed solution should uniquely identify and associate mitigation signatures with threat library content, by presenting a signature ID associated with each threat in the threat library.		
The proposed solution should present and classify signatures and mitigations by severity and category (web application attacks, vulnerability exploitation, malicious code) of the related threats.		
The proposed solution should allow the status of "not blocked" threats and signatures to be exported via CSV format.		
The proposed solution should allow signatures or threats to be searched and filtered using threat, action or signature names.		
The proposed solution should allow users to filter mitigation suggestions based on simulations.		
The proposed solution should allow users to filter non-tempering Malware Engine signatures to be shown or hidden on demand.		
For security gaps revealed during the web application and network infiltration assessments, the proposed solution should provide vendor-specific mitigation suggestions on a dedicated dashboard on the interface.		

For security gaps revealed during the Windows Endpoint Scenario and Email assessments, the proposed solution should provide generic mitigation suggestions on a dedicated dashboard on the interface.		
The proposed solution shall allow using "vendor severity" to filter signatures to prioritize and start mitigation actions.		
The proposed solution should be able to provide specific mitigation suggestions for the following network security solution vendors: a. Check Point (network intrusion prevention functionality) b. Cisco (network intrusion prevention functionality) c. Citrix (web application firewall) d. F5 Networks (web application firewall) e. ForcePoint (network intrusion prevention functionality) f. Fortigate (network intrusion prevention and web application) g. Imperva SecureSphere (web application firewall) h. McAfee (network intrusion prevention functionality) i. ModSecurity (Open Source) (web application firewall) j. PaloAlto Networks (network intrusion prevention) k. Snort (Open Source) (network intrusion prevention) l. Trend Micro (network intrusion prevention)		
Management & Security		
The proposed solution's Management should be able to operate both On-Premises and in an Air-Gapped Environment.		
The proposed solution should allow users to create custom dashboards for selected simulations.		
The proposed solution should assess Endpoint, Network and Email Security controls running on physical, virtual and cloud systems, via a unified Windows agent supporting Windows 10 and 11 Client OS versions and 2016, 2019 and 2022 Server OS versions.		
The proposed solution should assess Network and Email Infiltration, Data Exfiltration controls running on physical, virtual and cloud systems, via a unified MacOS 11 Big Sur, MacOS 12 Monterey operating systems running on Intel or M1 based processors.		
The proposed solution should assess Network and Email Infiltration, Data Exfiltration controls running on physical, virtual and cloud systems, via a unified Linux x86 and x64 based OS (Redhat 7, Redhat 8, CentOS 7, CentOS 8, Ubuntu 18.04+, Debian 9+).		

Heartbeat – The proposed solution should automatically verify the connectivity requirements among its attack components and immediately report any identified connectivity problems before each assessment.		
The proposed solution should allow setting up of each agent so that mitigation suggestions can be generated according to a list of vendor technologies.		
The proposed solution should have at least certificate-based, encrypted communication and authentication measures to secure communications among its software components.		
The proposed solution should be able to support the 2FA with Authenticator Apps.		
The proposed solution should support SSO (Single Sign On) with SAML (OCTA and Azure AD) and LDAP.		
The proposed solution should allow administrators to access Audit Logs via Web UI and analyze with filtering options.		
The proposed solution should allow administrators to configure Syslog Integration to forward Audit Logs via TCP or UDP to a log collector as CEF or JSON formats.		
The proposed solution should allow administrators to export Audit Logs via CSV file.		
The proposed solution should allow for the creation of multiple and customizable profiles - (i) admins, (ii) analysts and (iii) viewers with monitoring authorization levels only. Customizable options should be as follows: a. Simulations b. Templates c. Agents d. Custom Threats e. Custom Actions f. REST API Token g. Organization Management h. Mitigation		
Detection Analytics Module		
The proposed solution should have the ability to analyze whether the threats in the tested attack vectors are detected and alerted on "Security Information and Event Management" (SIEM) and Endpoint Detection and Response (EDR) solutions by connecting to the relevant solution platform(s).		
When connecting to the SIEM and EDR solutions, the proposed solution must provide a connection via" API "using username-password authentication or token.		
After the proposed solution has been configured for integration with SIEM or EDR solutions, it should be able to provide a warning in case of problems with access.		
When setting connectivity with relevant logging solutions to prevent failure and validate log data, the proposed solution should have a dedicated functionality to automatically test the accuracy and correct operation of user-defined queries.		

The proposed solution must have the required infrastructure that can be integrated with the following technologies: a. Chronicle SIEM b. CrowdStrike EDR c. Elastic SIEM d. Exabeam SIEM e. FortiSIEM f. IBM Qradar SIEM g. Logrhythm SIEM h. Logsign SIEM i. Micro Focus Arcsight ESM j. Microsoft Defender for Endpoint EDR k. Microsoft Sentinel SIEM l. Palo Alto Cortex XDR m. Rapid7 InsightIDR SIEM n. RSA Netwitness SIEM o. Securonix SIEM p. Sentinel One EDR q. Splunk SIEM (Onprem & Cloud) r. Trellix Endpoint Security (HX) EDR s. Trellix Enterprise Security Manager SIEM t. Trend Micro XDR VMware Carbon Black EDR (Onprem & Cloud)		
The proposed solution must provide an interface to determine when queries are made after the attacks are terminated. (Delay Time)		
The proposed solution must provide an interface to determine a time frame to compensate for small-time differences between agents and the management server. (Early Time)		
The proposed solution must provide an interface to limit the number of raw logs imported from SIEM to the management server to avoid high resource consumption on IBM QRadar and Splunk solutions.		
The proposed solution must provide an interface to define a limit on concurrent queries that can be made to the SIEM/EDR solution to perform detection analysis on parallel threats at the same time.		
The proposed solution should have an interface that can show MITRE ATT&CK framework coverage according to the detection results of Windows Endpoint Scenario attacks.		
The solution should report the total number of simulated threats logged, not logged, or alerted, not alerted for each simulation. A list of detection results for blocked and not blocked threats will be given.		
The proposed solution should support detection analytics outcomes to be displayed according to attack categories (File Download, Web Application, and Windows Endpoint Scenario Attacks).		
The proposed solution should provide an interface to visualize and compare the detection status in the last 7/30/90 days.		

The proposed solution should be able to show the prevention and detection status of any simulated threat on the same simulation result dashboard.		
The detection analytics, the proposed solution will be able to show the "start time" of the simulated attack, "the end time", "the time between two periods" and in addition, the "logging time", "the time between the end of the attack and logging", "the time between the end of the attack and the occurrence of the alert".		
The proposed solution should be able to output in CSV format for the purpose of reporting detected or not detected threats, and it should be able to show whether an alarm was raised following a simulated attack or not.		
The proposed solution should be able to output Threat Detection Results in a PDF report with logged or not logged, and alerted or not alerted threats.		
The proposed solution must have an infrastructure that checks whether "event data" that occur because of each attack simulation generate alerts.		
Alert results for the Endpoint Scenario Attacks should be matched with MITRE ATT&CK framework techniques and tactics by the proposed solution.		
The proposed solution should validate the events or logs collected from the systems it is integrated with (namely Log Management, SIEM or EDR solutions) to show those events or logs specifically related to each simulated threat and display it to the user.		
The proposed solution should be able to allow users to select whether to store raw detection log output from data sources. a. It should be possible to store raw logs. It should be possible to define the maximum number of raw log entries replied per query in each simulation.		
Detection Analytics Content		
The proposed solution should be able to provide Log Source Information to log necessary actions.		
The proposed solution should be able to provide Detection Content for following SIEM or EDR vendors: a. Arcsight ESM SIEM b. Carbon Black EDR c. CrowdStrike EDR d. IBM Qradar SIEM e. Microsoft Sentinel SIEM Splunk SIEM		
The proposed solution should be able to provide Detection Content as open-source SIGMA rules for other SIEM/XDR/EDR vendors.		
The proposed solution should allow users to view all rule recommendations for actions via a dedicated UI section. Solution should allow to filter “Not Alerted” actions.		
Reporting		
The proposed solution should report the total number of attack simulations executed, together with the number of blocked and not blocked attacks with, for		

each simulation. A list of total attacks blocked and not blocked will be given.		
The proposed solution should be able to export the vendor specific mitigation suggestions list with Signature ID, Signature Name, Vendor Severity, Not Blocked Action Count, Score Impact information in CSV (comma separated values) format.		
The proposed solution should provide a graphical interface to compare the security status changes in the last 7/30/90 days.		
The proposed solution should be able to enable users to generate custom reports, select content of the report and schedule them to be automatically sent to defined emails.		
The proposed solution should allow individual simulation reports to be generated for prevention and detection or only for prevention results in CSV and PDF formats on demand.		
The Solution should be able to export weekly and monthly executive and technical reports in PDF format.		
Monthly and weekly executive technical reports for all simulations in the system will be generated automatically.		
Users should be able to manage executive and technical reports' auto-generation preferences on Reports Settings for weekly and monthly reports.		
Users should be able to see the simulations that they are authorized to see in their reports.		
When weekly and monthly reports are created, users should be notified by mail. The people to whom the notification emails will be sent should be determined from the settings screen.		
Users should be able to generate reports from "Dashboard" and "Simulation History" pages.		
Users should be able to select simulations, report content (prevention, detection or both), report sections (from predefined sections) and edit report description in the report generation flow.		
The Solution should allow individual simulation reports to be generated for prevention and detection or only for prevention results in CSV and PDF formats on demand.		
The proposed solution should be able to share benchmark values for top 5 most simulated threat template results.		
The proposed solution should be able to share benchmark values for MITRE ATT&CK Tactics.		
The proposed solution should be able to notify users in Dashboard and via Email; a. When a simulation agent is down, b. When an integration agent is down, c. When an integration is unhealthy, d. When the overall score falls below or rises above a custom set threshold or defaults score change updates compared to 7 days ago.		

Attack Path Validation (Automated Pen testing)		
The proposed solution should be able to move laterally to achieve a defined objective by the admin.		
The proposed solution should be able to operate with both cloud and on-prem management platforms.		
The proposed solution must not require an agent to do the validation.		
The proposed solution should allow users to initiate the actions with following binary executables: a. Execution via New Threat Creation b. Execution via APC Injection c. Execution via Call-Back		
The proposed solution should have the following attack methods in this module: a. Lateral Movement b. Kerberoasting c. Local Privilege Escalation d. Harvesting and Spreading Actions		
The proposed solution should have the following harvesting actions available: a. Local Service Misconfiguration Enumeration b. Remote Management Users' Enumeration c. Session Enumeration d. LSASS Credential Dumping e. Domain Object Enumeration f. Domain DNS Enumeration g. Organization Units Enumeration h. Domain Trusts Enumeration i. Domain Service Account Enumeration j. Remote Desktop Users' Enumeration k. Distributed COM Users Enumeration l. Local Admin Enumeration		
The proposed solution should have the capability to evade its operations from security controls.		
The proposed solution should have the capability to export lateral movement findings as a CSV report with following information: a. Discovered Hosts (IP and Name) b. Discovered AD Group DNs c. Discovered Domain Users (Username and Password)		
The proposed solution should map the movement of the simulation in the GUI.		
The proposed solution should be able to show findings on the GUI while running the simulation.		
The proposed solution should be able to export simulation results in PDF or CSV format.		
The proposed solution should be able to export collected information per host as a CSV file.		
The Proposed solution should be able to provide generic mitigation suggestions for discovered security gaps.		

End-User Driven File Classification		
Ability to apply classification to Microsoft Office files - Word, Excel and PowerPoint		
Ability to show classification add-in in Office apps - Word, Excel and PowerPoint		
Ability to present users with guidance (tooltip) on classification labels in office apps - Word, Excel and PowerPoint		
Ability to suggest/recommend classification for Office files to the user based on keywords and pattern recognition		
Ability to seek justification from the users on downgrading the label or violating the suggestion		
Ability to prompt the user to mandatorily classify MS Office files - Word, Excel and PowerPoint		
Ability to apply bulk classification on multiple files in explorer		
Ability to change / update classification for files		
Ability to de-classify files		
Ability to automatically apply EDRM controls based on file classification label		
Language Support: Arabic, English		
End-User Driven Email Classification		
Ability to apply classification to emails within Outlook		
Ability to show classification add-in in MS Outlook		
Ability to present users with guidance (tooltip) on classification labels within Outlook		
Ability to suggest/recommend classification for emails to the user based on keywords and pattern recognition within Outlook email message and attachments		
Ability to seek justification from the users on downgrading the label or violating the suggestion		
Ability to prompt the user to mandatorily classify emails		
Ability to auto-upgrade email classification based on attachments		
Ability to change/update classification for emails		
Ability to de-classify emails		
Ability to automatically apply EDRM controls based on email classification label		
Ability to prevent user from sending emails to blacklisted domains		
Ability to allow users to send emails only to whitelisted domains		
Language Support: Arabic, English		
Granular EDRM Controls		
Restrict file access and usage to specific users and/or user groups		
Ability to provide read-only permission		
Restrict editing of files by unauthorized users		
Restrict printing of files by unauthorized users		
Restrict soft copy printing e.g., Print to PDF/Save as PDF		
Restrict copying content from a file to an external location		

Ability to provide full controls on files to specific users and/or user groups		
Restrict sharing of permissions by unauthorized users		
Restrict running macro on files by unauthorized users		
Block screen capture via PrtScr key or third party tools like SnagIt, Camtasia		
Block screen sharing via conferencing tools (e.g., Webex, GoToMeeting, etc.)		
Block file access via remote connections (e.g., Windows RDP)		
Block file access on virtual environments (e.g., VDI, Citrix environments, virtual machines)		
Allow file access while offline		
Restrict file access while offline		
Allow for different set of permissions for a user when he/she is accessing the file online vs offline		
Restrict saving unprotected copy with 'Save As' and other similar options		
Ability to save file in PDF format without the need to have full control permissions		
Enforce same set of controls when files accessed in native application vis-à-vis accessed online via browser		
Advanced EDRM Controls		
Restrict file access to a specific computer		
Restrict file access to a specific mobile device		
Restrict file access and usage based on date, time		
Restrict file access and usage based on number of days		
Expire all copies of a file remotely at any time		
Restrict file access to a particular IP address		
Restrict file access to a range of IP addresses		
Same level of security in collaboration with internal and external users		
Dynamic EDRM Controls		
Change permissions on a file after delivery		
Revoke access of users instantly and remotely		
Revoke access in real-time as soon as user gets online even though user has offline permissions on the file		
Replicate access of users instantly and remotely		
Replace access of users instantly and remotely		
End-user Driven Protection		
Protect one or multiple files simultaneously		
Ease of use - Right Click on a file/multiple files and enable protection		
Protect email attachments of any file format		
Enable different policies for individual users or user groups for the same file		
Allow usage controls to be saved as 'Policy templates'		
Ability to protect a file with one/multiple policy templates		
Enable protection on a file from within a native Office application		
Enable domain based protection/access for recipients		

Protect email body and attachments while sending emails via Outlook client on the desktop		
Set ad-hoc usage controls on email message and attachment in context to the email recipients i.e. users outside of the email recipient list should not gain access to the protected email and attachments.		
Protect attachments while sending emails via OWA		
Visual Markings and Classification Metadata		
Ability to apply visual markings like header/footer to MS office files and emails		
Ability to add classification metadata/x-header to classified files & emails		
Ability to preserve classification metadata even when the file is DRM protected for ease of interoperability		
Ability to preserve the metadata even on file conversion - i.e. MS office file is converted to PDF		
Ability to show an icon overlay for classified files, EDRM protected files		
Dynamic Watermarking		
Enforce watermarked viewing of protected files		
Enforce watermarked viewing of protected files even when the file is accessed in the native applications		
Enforce watermarked printing of protected files		
Ability to configure dynamic watermark content (Classification, date, time, username, etc.)		
Enforce watermark printing of protected files in browser		
Enforce watermarked viewing of protected files in a browser		
Display a combination of static and dynamic content in the watermark		
Display watermark on files accessed on mobile devices (iOS and Android)		
Customize the font and color of watermark content		
Automated Protection		
Automatically protect office files on close		
Automatically protect email body and attachments (from the server side) without any user intervention based on certain parameters like Sender, Recipient, Subject, metadata (x-header) tags		
Protect incoming emails and attachments from particular senders automatically without any user intervention		
Protect incoming emails and attachments from all senders to a particular email address without any user intervention		
EDRM Security for Email		
Send protected emails from Windows Outlook client		
Send protected emails from Mac Outlook client		
Send protected attachments from Windows Outlook client		
Send protected attachments from Mac Outlook client		
Send protected attachments from OWA		
Give permissions to distribution lists to access protected emails and attachments		

Ability for the recipients to automatically extend permissions on protected email and attachments to additional users		
Ability to set ad hoc security on emails and attachments for the recipient list only		
Track protected emails and attachments from within Outlook itself		
Revoke access to protected emails and attachments from within Outlook itself		
Set expiry date for protected emails		
Protect incoming emails and attachments automatically without any user intervention		
Encrypt and Decrypt .pst files		
Track audit logs for decrypted .pst files		
Automatic protection of emails based on custom metadata/tag/label fields tagged by 3rd party systems e.g., Discovery, Classification, and DLP systems		
View protected emails (body and attachment) from the browser on your desktop – without the need for a particular email client or software		
Reply to protected emails from the browser on your desktop or mobile – without the need for a particular email client or software		
Authentication		
Ability to authenticate users via Windows Active Directory		
Ability to authenticate users via Microsoft Azure Directory		
Ability to authenticate external users with their personal or work account		
Single sign-on (SSO) capabilities with Google		
Single sign-on (SSO) capabilities with Microsoft Azure		
Works with other identity/SSO solutions like Ping, Okta		
Ability for external users to access a file with a temporary one-time password (OTP) without creating an account		
Support for 2FA with time based OTP (TOTP)		
Support any authentication providers with OpenID Connect protocol		
End-user experience with EDRM Files and Emails		
View protected files online on Windows and Mac desktop platforms without installing any software		
Edit protected files online on Windows and Mac desktop platforms without installing any software		
View protected emails online without installing any software or depending on any particular email client		
Reply to protected emails online without installing any software or depending on any particular email client		
Open protected files in native applications		
Access to files according to permissions set by the file owner		
Unprotect files on desktop for users will permissions		
Open protected files online directly from SharePoint Online, OneDrive, and Teams		

Open protected files in native applications from SharePoint Online, OneDrive and Teams		
Access protected files on any browser		
Access protected files on any device (Windows OS, MacOS, iOS, Android)		
No dependency on OS to access protected files/emails on desktop or mobile devices		
No dependency on application license to access protected files/ emails on desktop or mobile devices		
External users can access protected common non-office formats like PDF, png, jpeg, txt, etc. without installing any specific tool or software		
Support for Dynamic Watermark viewing		
Ability to extend permission on protected files/emails		
Ability to automatically extend permissions on email and its attachments on 'Email Forward/Reply/Reply All' to any new recipient added without the need to do anything outside of the context of sending the email		
Ability to request for permissions on protected files/emails		
Access protected files with Save-back functionality from within the integrated app to avoid/reduce the need for file download		
Seamless and consistent external user experience with protected emails and/or files		
Security widget within the file to display the usage permissions for a user on the protected file		
Administration - General		
Segregation of duties: Support for different administrator roles based on scope of work		
Ability to create security admin user profiles		
Ability to create power users (business users) for managing groups		
Ability to view installation report detailing agent installations throughout the organization		
Centralized license management for admins		
Ability to auto-assign license based on usage		
Customized user interface with your company’s logo		
Administration - Classification Policies		
Must offer an Admin GUI for classification policy administration		
Ability to define and configure classification label list		
Ability to define color for different classification labels		
Ability to define a tooltip for each of the classification labels		
Ability to define sub-labels for a classification label		
Ability to define font size, color, text alignment for Header, Footer visual markings		
Ability to configure EDRM protection policies for a classification label		
Ability to define blacklisting of emails domains		
Ability to define whitelisting of email domains		
Ability to define priority for classification labels		
Ability to create exceptions (for a certain set of users) against the label policies		

Ability to configure content discovery policies based on keywords and patterns		
Ability to publish classification labels to users, user groups		
Ability to configure default classification in Office apps and Outlook		
Ability to configure mandatory classification for documents and emails		
Ability to publish classification for documents or email or both		
Ability to enable/disable classification via in-app menu within MS Office apps - Word, Excel, PowerPoint, Outlook		
Ability to enable/disable classification via right click menu option in explorer		
Single GUI to manage and administer Classification and EDRM policies		
Tracking		
Instant email alerts to file owners for unauthorized file activities performed by users on EDRM protected files		
Daily digest email sent to file owners summarizing all the day's activities on protected files		
Ability to track and revoke access to EDRM protected files, emails for internal users		
Ability to track and revoke access to EDRM protected files, emails for external users		
Ability to revoke access for a specific user/user group		
Reporting		
A web-based audit trail and dashboard for all EDRM activities performed on all files by all users		
Report builder tool for easy custom reporting based on user needs		
Ability to log forensic details - Name, Email ID, IP Address, Device, Machine name, file location on users device, Allowed and disallowed operations		
Ability to log date/time on which the activity was performed by the user		
Ability to export activity logs for monitoring purposes		
Ability to export audit logs for regulatory compliance reporting		
Ability to provide unified view of major risk and usage parameters		
Monitor license utilization		
Ability to provide overall system health and utilization/adoption analytics		
Ability to import/publish logs into SIEM tools		
A web-based audit trail for all classification activities performed on files and emails by users		
Report builder tool for easy custom reporting based on user needs		
Ability to log date/time on which the activity was performed by the user		
Dashboards		

Solution must offer a centralized dashboard for executive reporting via Insights into Risks - Present and Averted		
Solution must offer a centralized dashboard for executive reporting on EDRM protected data		
Solution must be able to show trends over a period of time for Risks		
Solution must be able to show trends over a period of time for EDRM protected data		
Solution must be able to show a map-based view for risky activities performed		
Solution must be able to show a map-based view for risky activities prevented		
Solution must be able to show unauthorized activities performed based on domain of users		
Dashboard for EDRM protected data with filters on time-period		
Centralized dashboard for executive reporting via Insights into Risks - Present and Averted		
Solution must be able to show trends over a period of time for Risks		
Operating System Support		
All major Windows versions		
All major MacOS versions		
iOS devices		
Android devices		
File Formats and Applications Support		
Microsoft Office files: doc, docx, xls, xlsx, ppt, pptx, docm, pptm, xlsm		
PDF files		
txt and other ASCII-based files		
OpenOffice formats: odt, ods, odp, odf, odg		
Image files: jpg, jpeg, bmp, png, gif, tiff		
All major Microsoft Office versions: 2016, 2019, and Microsoft 365		
All major OpenOffice versions: 4.x		
All major Adobe Reader versions: XI, DC		
All major LibreOffice versions: 6.x		
All major Windows versions: 8.1, 10		
Deployment and Customer Support		
Availability as a hosted service in cloud		
Availability to deploy on-premises		
Ability to deploy in hybrid mode		
Single agent/client for Digital Asset Classification		
Silent installation of agent via central deployment tools for Windows and MAC		
Support for cloud-based system in a private cloud		
Support for seamless migration from cloud-hosted to on-premises deployment		
Support for automated patching of apps using app stores		
Support for automatic and silent client upgrades		
Availability of different modes of agent i.e. Protection mode and Receiver mode		
Availability of 24x7, SLA-bound support		

Data Classification professional consulting services		
Access to delivery and on-going account management team for successful roll-out and on-going adoption of the technology		
Network Detection & Response / Mandatory Requirement		
Detect Performance and Scalability		
The solution must have a very high scalable platform that can support different options for sensors and analyzers/brains, supporting up to 75Gbps in a one rack unit analyzer with the different sensors types (Virtual, Physical) and sizes (1,15,20,50 Gbps) connecting to the same console/brain.		
The solution must have the option to deploy sensors for the virtual environments such (Vmware ESX, Hyper-V, KVM)		
The solution must be passive to the network i.e. not taxing network performance.		
The solution must operate effectively and efficiently in an air-gapped environment without external influence i.e. people or other technology.		
The detect must be agentless (no agent to be used for any purpose).		
The solution must not require traffic decryption.		
The solution must have capability to use one rack unit server that is working as sensor and brain to process the traffic.		
The solution must have one server with 4 ingest ports which allow to ingest traffic from 4 ports..		
The solution must be able to store the detections in the the brain.		
Detect Analysis and Automation		
The solution must automatically identify and classify threats, including attack phase and risk, without requiring any manual work to build/tune the use cases		
The solution must have a AI Triage Advisor page to create triage rules automatically using machine learning and AI.		
The solution must be behavioral based only (signatureless).		
The solution must differentiate key assets from other hosts for risk prioritization.		
The solution must possess a mechanism to automatically show the confidence of detection when threats are detected based on anomalies		
The solution must have single dashboard for detections that correlates multiple networks detections together automatically		
The solution must have host quadrant severity that shows two values (certainty score and threat score).		
The solution must be able to automatically differentiate between general botnet behaviors and those that are more likely to be targeted threats.		
The solution must be able to detect botnet behavior including DDoS, external vulnerability scanning, Bitcoin mining, etc.		
The solution must be able to detect hidden tunnels within HTTP, HTTPS, and DNS used for command-and-control and data exfiltration.		
The solution must be able to detect the use of algorithmically generated domains or DGAs		
The solution must be able to detect custom RATs (remote administration tools) from normal user traffic		
The solution must be able to detect unknown command & control (no reputation history) using other traffic attributes		
The solution must be able to detect data exfiltration independent of user identity or IP address		

The solution must be able to detect internal reconnaissance of an attacker		
The solution must be able to detect reconnaissance using slow or “paranoid” network scans		
The solution must be able to detect improper use of administrative and management protocols, including RDP, SSH, iDRAC, and IPMI		
The solution must be able to detect activation of sub-OS rootkits using port hijacking		
The solution must be able to detect remote execution of procedure calls or code via SMB or DCERPC protocols		
The solution must be able to detect privileged access analytics use cases by observing the privilege for the (account, host and service).		
The solution must be able to detect automatically re-categorize behaviors that are caused by approved systems or usage, e.g. network scanners		
The solution must be able to detect advanced C&C detection is the foundation		
The solution must be able to detect all hosts that have connected to the C&C infrastructure		
The solution must be able to detect highlight relevant lateral detections between hosts		
The solution must be able to detect attacker activity across multiple hosts to give comprehensive campaign view		
The solution must be able to automatically identify and outline attack campaigns		
The solution must list all user accounts and show two main metrics (threat score certainty score)		
The solution must use AI to do the Triage and eliminate the manual work from the security teams and saving time and help the security teams to focus on what matters.		
Detect Prioritization and Investigation of Threats		
The detect must automatically score and prioritize each individual detection.		
The solution must automatically score and prioritize each host based on its behaviors over time (focus on attacker progress prioritization not just single event prioritization using AI & machine leairning)		
The solution must automatically score and prioritize each user account based on its behaviors over time (focus on attacker progress prioritization not just single event prioritization using AI & machine leairning)		
The solution must use AI & machine learning to do the prioritization based on attacker progression over the time.		
The solution must be able to notify staff based on the threat score		
The solution must provide elevated visibility of key assets with identified attacker behaviors		
The solution must provide individual scores for both threat and certainty / confidence		
The solution must provide visibility into host interconnectivity		
The solution must provide packet captures of identified attacker behaviors for analysis		
The detect must find commonalities across multiple devices in the network and present it in a coherent attack campaign of all hosts participating in the campaign		
Detect Methodology		
The solution must directly identify threats based on network traffic analytics and depend on the behavioral models to find unknown without the need to decrypt the traffic.		

The detect must cover more than 97% of the MITRE ATT&CK network based attackers tactics		
The company must have patents published in MITRE D3FEND.		
The solution must detect network-based threats within encrypted traffic without the need of decryption		
The solution must detect custom or unknown threats, where there is no signature or IP/domain reputation history based on behavior		
The solution must focus on attackers behaviors (TTPs) not just simple anomaly models with generic ML approach.		
The solution must cover all infrastructure devices (Windows, Mac, mobile devices, BYOD, IoT, routers, firewalls)		
The solution must use multiple behavior techniques (Supervised Learning, Unsupervised Learning, Deep Learning).		
The solution must analyze and correlate all network traffic direction: (North, South) and (East, West) traffic.		
The solution must secure the data center within the virtual environment as well as the underlying infrastructure		
The solution must use Stream to forward metadata into external storage to make threat hunting and more investigation.		
The solution must allow to upload STIX file for signature detection.		
The solution must learn automatically the Privileged Access Analytics for (host, account, and service privilege).		
The solution must use observed privilege to strengthen zero-trust access.		
Modeling of Threats		
The solution must incorporate global attack behaviors and techniques to detect threats on the local network.		
The solution must use global modeling of threats to be combined with local network learning to improve accuracy and relevance for the local network		
The solution must detect potentially-malicious anomalies based on deviation from learned local norms within the network		
The solution must detect threats within new devices or devices that were already compromised when baselined		
The solution must not use a generic approach to build its unsupervised models		
Analysis		
The solution must maintain network packet captures PCAP of detected attacker behaviors		
The solution must not depend on NetFlow/logs as a data source only.		
The solution must use raw network traffic (PCAP) for real-time analysis		
The solution must utilize Artificial Intelligence capabilities to augment and automate SOC operations		
The solution must create shareable link from the UI interface for specific detection to be shared with a user who does not have an account on the UI interface		
The solution must allow to Tag the host from the UI interface.		
The solution must allow to create a Note on the host and account from the UI interface.		
The solution must allow to assign a user to specific detection to start analyzing it without requiring to have an account on the UI interface.		

The solution must support access and search using RESTful API.		
Types of Threats		
The solution must detect remote access tunnels used by attackers to control compromised systems		
The solution must detect hidden tunnels over HTTP, HTTPS, or DNS to communicate with C&C or to exfiltrate data		
The solution must detect web-based Command and Control (not relying on IP reputation or threat lists)		
The solution must detect malware using a fake browser		
The solution must detect multihomed domain fronting.		
The solution must detect relay hosts.		
The solution must detect malware getting new instructions		
The solution must detect malware replicating a payload to / exploiting vulnerabilities against other hosts		
The solution must detect TOR anonymization		
The solution must detect peer-to-peer traffic		
The solution must detect Botnet monetization behaviors: Click Fraud, Bitcoin Mining, outbound DoS, outbound SPAM		
The solution must detect ransomware activity: encrypting file shares		
The solution must detect network reconnaissance scans: port scans, port sweeps, scanning unused IPs.		
The solution must detect privilege anomaly like Privilege escalation, accounts take over, credentials theft and misuse.		
The solution must detect the use of a stolen credential from its normal system, but asking for unusual services or in excessive volume		
The solution must detect a host trying many credentials to attempt to gain access to a server		
The solution must detect Kerberos service scans		
The solution must detect fake Kerberos servers		
The solution must detect brute force attacks		
The solution must detect RPC reconnaissance		
The solution must detect the use of administrative protocols, including RDP, SSH, IDRAC, and IPMI, where the target host is not typically administered by the source host on that protocol		
The solution must detect activation of a sub-OS rootkit using an "knocking" byte sequence on a common port		
The solution must detect a host gathering unusual volumes of data and then sending exfiltrating to an external IP		
The solution must detect a host being used as a relay to exfiltrate data to an external system		
The solution must detect enumeration of file shares		
The solution must detect AD/LDAP reconnaissance using techniques similar to Bloodhound		
The solution must detect use of PowerShell/WMI and RPC to move laterally via remote code execution		
The solution must detect use of stolen RDP client tokens		
The solution must detect reconnaissance of RDP servers		
The solution must detect reconnaissance of RPC servers		
The solution must detect the use of PS exec and other remote administration tools to move laterally via SMB		
The solution must detect a host being used as a relay for command and control purposes to gain access deeper into the network		
Integrations and Response		
The Detect must natively integrate with EDR vendors like Microsoft Defender ATP, Carbon Black , FireEye, SentinelOne, Cybereason and CrowdStrike.		

The solution must have an option to lock down host and user accounts manually by pressing a button in UI interface.		
The solution must have an option to lock down host and user accounts automatically by integrating with SOAR solutions.		
The solution must able to ingest traffic from TAPs solutions.		
The solution must provide API-driven access to all events, hosts, and scoring information for integration with other security solutions (NAC, SOAR, FW, EDR) & ticketing systems.		
The solution must integrate with AD to lock down user account by surgically freeze account access and avoid service disruption by disabling accounts (auto and manual)		
Operations		
The solution must have automatic update to reduce the operational burden of the solution.		
The solution software must be updated with a regular frequency to adapt to the constantly evolving threat landscape.		
The solution must provide appropriate commentary around the detection including appropriate triggers as well as steps to verify and where to begin potential remediation.		
The solution must enrich its metadata/detections/hosts with the info that will help improve the IR approach, natively and without complex integrations (Host ID)		
The system must meet all the requirements without using any VPN or cloud connection.		
The solution must not send any data outside the organization or using any cloud processing.		
The solution must be able to provide health monitoring via email and syslog.		
The solution must be able to show health monitoring in UI interface.		
The solution must be able to alert on individual threats or suspicious hosts via email and syslog		
The solution must provide granular role-based access control (RBAC) into the various elements of the product so security analysts can define custom roles with limited access if desired		
The solution must have the ability to send audit log over syslog for actions such as login, logout and changes to settings that impact the security posture of the product		
The solution must provide quarterly health check from the vendor		
The solution must have NDR references in government sector ,Oil/Gas and Finance inside Saudi Arabia		
The NDR vendor (not the local partner) must have local team members in KSA for implementation and support.		
The license must be based on number of IPs, not based Throughput		
Training		
The course must cover the use of Detect for SOC analysts.		
This course must help students to the use of Detect to discover behaviors and attacks and to optimize workflow.		
The course must covere Detect overview; UI walkthrough, configuring triage rules for recurring behavior, reports, email alerts, syslog forwarding, and user management.		
The course must be at least 2 days.		
Support		
The solution must provide Premium Support using web portal and email support.		
The solution must provide knowledge base access.		

Device and License Installation		
The solution installation must include sensor devices and Brain.		
The solution must include Detect solution and license installation.		
The installation must include traffic analysis (topo).		
The installation must include one triage session.		
The installation must include sensor and Brain communication and configuration.		
The license must be software subscription and support per active IP.		
Sensors		
The vendor must have a scalable platform that can support different options for sensors and brains, supporting up to 75Gbps in a one rack unit analyzer with the different sensors types (Virtual, Physical) and sizes (1,15,20,50 Gbps) connecting to the same console/brain.		
The solution must have capability to use one rack unit server that is working as sensor and brain to process the traffic.		
The solution must be available with X29 type sensors		
The solution must have one server with 4 ingest ports which allow to ingest traffic from 4 ports..		
The sensor must have two management ports with 1 Gbps.		
The sensor must have ability to ingest 15 Gbps traffic in one device.		
Total cost of ownership		
No need to move infrastructure to cloud e.g., On-Premises AD to Azure AD, On-Premises exchange to exchange online, etc.		
No need to upgrade infrastructure to latest versions e.g., Windows 10, Microsoft O365, etc.		
Key Management		
Protected content and keys are kept separate for hack-proof security		
Pluggable encryption: Bring your Own Encryption		
Keys are never embedded within the protected file		
Reporting & Analysis		
Out of the box reports		
Customized reporting		
Reports via subscription		
Privilege risk dashboard		
Analysis of privilege use across endpoints		
Analysis of privilege sprawl over time		
Authentication		
Access to the system must be controlled by a log-on procedure incorporating individual user identifiers and passwords.		
The solution must restrict target-account-specific entitlements of end users individually or by group or role		
Solution must contain up to three tiers of approval		
Supports contextual zero trust by making secondary MFA authentication mandatory when selecting sessions.		
Support built-in access certification		
Integration		

Removing application-to-application hardcoded passwords.		
Allow sessions to be started via any SSH or RDP client		
Integration with Microsoft LAPS		
Third-party vault integration		
Architecture		
The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.		

ملحق (٣): متطلبات ومعايير هيكلية تقنية "Enterprise Architecture Requirements"

#	Category	Item
١	General Architecture Requirements	The deployed components (such as processes or technologies) shall be standardized/ adhered to best practices. Customization should be kept to a minimum while deploying.
٢		The deployed components shall be configurable, and maximum level of customization recommended by providers should not be exceeded.
٣		The deployed components shall fit the business purpose and be aligned with Enterprise Business Target Operating Model and strategy.
٤		A component should be used for which it was originally developed for. Best practices, COTs (Commercial off the shelf) standards, and IT related Frameworks - where fit - shall be used to develop IT Solutions to enable IT Services.
٥		Each component (processes, data, applications, services, technologies and platforms) shall be documented, and the documents shall be kept up to date for any evolution or update on the components.
٦		Each component must be secured against unauthorized access.
٧		Each technology component should be scalable vertically and horizontally.
٨		Technological diversity should put in control while preventing vendor lock in technology provision.
٩		Acquiring new IT components shall be governed by Enterprise Architecture. The acquirement of new IT Components shall be justified.
١٠		Decision should be taken to decommission any IT component if no longer serving business needs or if its cost of support and maintaining is higher than acquiring and migrating to new assets that fit the purpose.
١١		The licenses should be managed to only pay for what will be utilized.
١٢		Technology should be a leader in its domain and should be obtained from a financially stable vendor. A Well-established Open-Source product can be considered given that it is a leader in its domain, and a continuous enhancement to that product is owned by a leading vendor in addition to the support and maintenance. When obtaining an Open Source Product, no modification is allowed in the source code of the product until it is very well negotiated and approved by the vendor, and the vendor confirm it will be considered in the product future releases.
١٣		Enterprise Architecture maintain and update an approved list of technology vendors, and any exception to this list should be approved first by Enterprise Architecture management.
١٤		Technologies and solutions shall be Obtained and implemented while focusing on enabling Business for MoD and considering military trends and new aspects. IT Services/Infrastructure shall be defined from the Business perspective and best practices, not based on the IT technology deployed to deliver that service.
١٥		Measurement of IT Service performance should be relevant to Business impact and value. Reporting of service performance should clarify business impact.
1	Digital Architecture Requirements	IT initiatives shall concentrate and move toward achieving MoD digital mission and needs.
2		IT services should be offered through easy to use web enabled access and responsive multi-channel interfaces while ensuring Omni channel.
3		APIs exposure should be considered when designing the eServices and should be exposed by developed services.
4		Digital related initiatives shall understand MoD user characteristics, users' culture and behaviour to better address their digitalization needs, and should enable user feedback and input throughout the digitalization lifecycle.
5		The solution should enable the Contextual feature in the digital channels such as user preferences, location, personalized interactions and services through application of data analytics and insights.



6		The solution shall ensure privacy, security, and ethical use for the users' data through digital channels.
1	**Infrastructure Architecture Requirements**	Technological diversity should be controlled as the cost of integration between various technologies has to be considered. Technology adoptions will be constrained by the approved technologies.
2		Technology components should adopt the state-of-art technology to utilize new adapted technology trends, ensure long term support and Return on Investment (ROI).
3		The technology components should support interoperability, adaptability, portability, and scalability.
4		Infrastructure components must support availability targets to minimize downtime for mission critical applications. DR concept should be available for mission critical applications/services and should support Recovery objectives.
5		Data shall be stored in reliable infrastructure, be backed up and archived using leading solution and according to defined policies.
6		Technology architecture should consider Virtualization and Containerization when developing the architecture.
7		The technology should support the transfer to cloud-based services.

#	Category	Item
1	Application Architecture Requirements	Re-use Before Obtain Before Build, for new business requirements, the vendor should consider first reusing existing technology capabilities. If not applicable (such as huge customization is necessary to fulfil the new requirements, or existing technology does not have the necessary capabilities, or such will violate Architecture requirements and IT Standards) then consider obtaining new technology, if the market cannot provide such solution, then apply in-house build to satisfy such needs.
2		Service oriented approach (SOA) should be adopted in acquired Solutions to improve reusability and reduce duplication, these solutions will have loosely coupled components that can be referenced across multiple applications.
3		Enterprise Service Bus (ESB) shall be used to decouple applications from specific software solutions.
4		Microservices should be used when there is a need for agile application that demand high delivery speed, the application is big enough to justify the use of Microservice, Application domains are clear and linked to business to micro-service them, and Infrastructure and technical team are ready to operate such environment.
5		Solution should support layered architecture, for example, separate presentation layer from business logic layer and data layer.
6		The vendor should follow a well-recognized and best practiced development methodology when developing a solution.
7		The Developed or acquired IT solution should address existing requirements and expected future needs, and should have a broader view than a single application-based solution. The solution should have a broader view and should consider integration with existing solutions.
8		Acquired technologies shall not be vendor locked, where vendor capabilities will constraint MoD strategic improvement and future priorities.
9		Applications should be user friendly. The underlying technologies must be transparent to the users.
10		Adapt common look and feel user interface, ensure easy to use interface, Applications should enable easy switching between different languages, particularly English and Arabic, and support internationalization and localization. The solution should allow the alteration of its behavior without resorting to code change.
11		An appropriate on-line and offline documentation should be available to guide users and to help solve problems.
12		The Application shall enable the IT Operation to measure, document, and report its availability and performance.
13		Application should be fault tolerant with error handling capability.
14		Application should be available from customer perspective in the frame of agreed service levels: the availability targets should be defined from user perspective and according to system criticality.
15		Application activity should be traceable through history of operation transactions, audit logs, and error logs.
16		MoD IT Target Architecture will be used to guide the decision of technologies adoption for business functionalities. This is to: Ensure the alignment with industry standards and best practices, • Ensure agile and cost-effective Architecture, • Provide unambiguous decision of the required capability for each functionality, • Prevent capability overlap of IT Applications, • Identify capability gaps.
1	Data Architecture Requirements	Data has to be managed as an asset that has value to MoD. The business should have access to the right information at the right time to enable making the accurate decisions.
2		Information model and common data dictionary should be used for business, operational and technical views. Naming rules should be followed to create new data entities.
3		The data shall be maintained in central environment and shared according to business relevancy.
4		It should be specified which application type components in the landscape will serve as the system of record or reference for enterprise master data.
5		The IT solution shall ensure confidentiality, integrity and access control while sharing Data. Data sources shall be maintained through CRUD matrix.
6		The movement of information between users and systems shall be captured efficiently. Lack of knowledge of information flows will lead to duplicate integrations and inappropriate decisions on how to satisfy information consumers.
7		Data should be retained according to MoD regulations and data policies.
8		Archiving and retention policies should be defined per information entity.
9		MoD IT Target Architecture shall be used to guide the decision of Data blocks definition and modelling to enable business functionalities.

#	Category	Item
1	Integration Architecture Requirements	Integration between systems should utilize standardized technologies and built-in APIs whenever possible.
2		Enterprise Service Bus shall be used for any communication between the Business applications.
3		API Gateway shall be used by external consumers for any business application.
4		Applications and modules should expose built-in APIs to enable systems integration.
5		The APIs shall support mainstream programming languages.
6		Customization of API is not allowed unless necessary and approved by Enterprise Architecture.
7		Integration between systems shall use standard technologies (such as REST).
8		The services should be linked in a loosely form to enable process, in which, no interdependence between individual services are there.
9		Seamless integration should be allowed for external systems with MoD systems: the integration architecture shall be designed so that any changes required to deal with new changes in external systems are as least disturbing as possible.
10		Service Oriented Architecture (SOA) approach shall be used to generalize the service case with the consideration of dynamic configurable scalability to promote the service re-use.
11		Service interface and implementation specifications should be in a registry to enable services search and to eliminate the possibility of overlap between services.
12		Integration layer shall maintain unique ID for each process execution for the purpose of tracking all systems activities related to the process execution.
13		Integration patterns/methods shall be defined based on best practices.
14		Each API shall have declared purpose, specified consumer(s), and Identification of the granularity level of the API.
15		APIs versioning shall be managed to ensure compatibility and flexibility.

ملحق (٤): معايير البنية التحتية

#	Category	Item
١	)Common Compute Requirement (High Dense server farm	The solution should comply with the industry definition of Composable Infrastructure; where the physical compute, storage and network (compute) fabric resources can be assembled and configured in various combinations to improve the efficiency and accelerate application serviceability.
٢		The solution should provide resources that are logically pooled so that administrators don't have to physically configure hardware to support a specific software application. Instead, the software's developer defines the application's requirements for physical infrastructure using policies and compute profiles.
٣		The composable solution should be able to provide internal and external storage simultaneously using industry standard protocols
٤		Internal (DAS, SAN, iSCSI)
٥		External Storage (FC-SAN, iSCSI, NAS etc)
٦		The solution should support the use of application programming interface (API) to create (compose) the infrastructure it needs to run on bare metal, as a virtual machine (VM) or as a container.
٧		The offered solution be able to optimize any application and store all data on a single infrastructure with fluid pools of physical and virtual compute, storage, and fabric.
٨		The proposed Solution should be based on blade server enclosure/chassis architecture.
٩		The enclosure (itself) should provide consolidation of compute, fabric and storage resources.
١٠		The proposed solution's enclosure/chassis should support half-height, full-height or full-height double-wide compute modules. This would ensure the solution can run any kind of workload and better VM density in case of virtualized workloads.
١١		Vendor will have to make sure that all the components within the proposed solution are tested to work together and there should be no compatibility or interoperability issues between the hardware (compute, network & storage) and software components (management, hypervisor, OS, software defined compute & storage elements) or the solution.
١٢		Vendor will have to make sure that the firmware and driver versions are fully compatible and tested with the proposed solution.
١٣		The solution should have the ability to flexibly scale up and scale down as the workloads dictate and precisely align operating expense to actual usage.

#	Category	Item
١٤		Proposed solution should be able to host/provision traditional applications (bare metal/virtual) that are designed to support and automate existing business processes such as collaboration, data processing and analytics, supply chain, and web infrastructure.
١٥		The solution should be able to host/provision new breed of applications and services which drive revenue and new customer experiences by leveraging Mobility, Big Data, and Cloud Native technologies.
١٦		The solution (as a one infrastructure) should be able to host Virtualized, bare-metal, containerized and hyper-converged (based on software-defined-storage) workloads. The actual requirement of hosting different servers in a single enclosure/chassis may vary and could span on multiple enclosures/chassis. However, vendor should offer the solution in the best consolidated manner.
١٧		The solution should be able to host variety of compute nodes/servers (homogenous and heterogeneous within a single enclosure) having 2-socket or 4-socket CPU architecture. This would ensure better VM density (in case of virtualization) compared to a homogeneous 2-socket processing node. This would also provide better consolidation within the datacenter.
١٨		Vendor should clearly mention the throughput or backplane capacity of the enclosure/chassis.
١٩		The proposed enclosure/chassis should support interconnect/switching modules with active/active or active/backup network connectivity.
٢٠		The proposed system's bandwidth and throughput should be aligned with the bandwidth (Ethernet, FC/FCoE & ISCSI) required per server and there should be no bottle neck in the architecture.
٢١		Blade Server Speciation
٢٢		Dual Sockets and four socket with the following specifications:
٢٣		2 or 4 x Intel Xeon Cascade lake or newer
٢٤		Each CPU should have 24-cores with the base frequency of 2.1GHz and 45M cache.
٢٥		576 GB of DDR4 RAM on each server expandable up to 3 and 6 TB respectively
٢٦		Vendor should mention the scalability of the memory and CPU on each blade server
٢٧		Each blade server have one Converged Network Adapter with 2 x 25/50G CNA ports.
٢٨		For future upgrades blade server should support additional CNA ports or HBA ports
٢٩		Each network card (CNA) should support physical or virtualized functions for the ease of management and better data throughput.
#	**Category**	**Item**
٣٠	)Common Compute Requirement (High Dense server farm	The enclosure should provide a composable physical storage module/node which should be able to provide direct attached storage or shared storage space to the compute nodes internal or external to the enclosures.
٣١		The storage module should support large disk configurations and should be configurable for different workloads. (Virtualized as well as bare metal). Any number of drive bays in a storage module can be configured with any compute node, allowing for efficient utilization of available drives.
٣٢		The storage module should be configurable as direct attached storage and as a Hyper-Converged storage (software defined storage) simultaneously.
٣٣		Bare-metal and virtualized workloads (servers) should be able to access the storage module directly (zoned drives) or via software defined storage (as Hyper-Converged solution) simultaneously.
٣٤		The storage module should provide complete storage array functionality for virtualized environments and should provide the basis for turnkey iSCSI storage consumption with iSCSI offload support in a huge number of CNAs.
٣٥		In case of virtualized environment the solution should support industry leading hypervisors (VMware, MS Hyper-V, Linux KVM).
٣٦		In case of virtualized workloads, the storage solution should be certified/qualified with VMware Compatibility Guide, Microsoft Windows Server Catalog, VMware Site Recovery Manager VMware Metro Storage Cluster etc. Vendors are open to mention the equivalent capabilities provided by the proposed solution. It is vendee's discretion to use the suitable feature as per the business requirements.
٣٧		The storage module should support hypervisor based advanced features such as vMotion and Live Migration without purchasing external storage system.
٣٨		Keeping in mind of the future expansion, vendor should clearly mention the expansion capability of the storage module(s) within the enclosure.
٣٩		The storage module should offer the expansion via multiple drive types (12G SAS or 6G SATA HDD and SSD Smart Drives) to be configured in the same storage module. It should support mixing of different drive types (SAS/SATA, SSD/HDD) and sizes in a single enclosure.
٤٠		In case of hybrid disk drives in a hyper-converged solution, the storage solution should optimize data (frequently accessed tier/non-frequently accessed tier) transparently between different storage tiers.
٤١		The enclosure or the compute architecture must have embedded fabric architecture which should be configured as part of the composable infrastructure.
٤٢		The system must support an architecture that can be spread over multiple racks, ensure there is a pre-engineered network design and the whole system are managed as one product.

#	Category	Item
٤٣		Network connectivity between multiple cabinets as the solution should be able to spread across several racks. The solution should optimize east-west traffic and should enhance the application performance by providing clustering between the nodes/enclosure/chassis without the need of having top-of-the-rack switches.
٤٤		Network resources should allow granular configuration and allocation of bandwidth to compute resources (VMs or OS).
٤٥		Network configuration should allow dedicated quality of service within the compute resources; this should be in addition to the network (physical switch based) quality of service. This would ensure optimized east-west traffic and better application serviceability.
٤٦		The proposed architecture must support out-of-band management solution. True and end to end Out-of-Band Management is a must requirement as it allows to manage infrastructure during security problems, Routing and Spanning Tree Protocol loops and Denial of Service attacks. In case of network attack the operations team should have network access (GUI, CLI) to the overall stack.
٤٧		The compute fabric (network) should offer disaggregated, rack-scale design architecture to consolidate data center network connections, reduce hardware and management complexity, and scale network bandwidth across multiple enclosures.
٤٨		Interconnect/Switching module should support Ethernet as well Fiber Channel connectivity using a single module.
٤٩		Each switching module should support minimum of 600Gb of uplink bandwidth and 600 Gbps of downlink bandwidth (internal server connectivity). Each downlink port can be carved up (physical) into multiple ports (Ethernet, FC), and the administrator should be able to configure separate downlink speeds using Ethernet or FC protocols or both simultaneously. This provides the administrator to control the bandwidth availability for the operating system/application.
٥٠		The network interface card (converged network adapter) on the compute nodes should support following functionalities:
٥١		IEEE quality of service (QoS) 802.1p tagging
٥٢		IEEE 802.1Q virtual local area network (VLAN)
٥٣		TCP, IP, UDP checksum offload, Large Send Offload (LSO), TCP, Segmentation Offload (TSO)
#	**Category**	**Item**
٥٤	)Common Compute Requirement (High Dense server farm	It should support overlay networking on host performance with tunnel offload support for VXLAN and NVGRE
٥٥		It should support Single-Root I/O Virtualization (SR-IOV) which provides a mechanism to bypass the host system hypervisor in virtual environments providing near metal performance and server efficiency.
٥٦		The network interface card should be configured as part of the stateless computing profiles.
٥٧		The downlink should support Ethernet, Fiber Channel over Ethernet/CEE or Accelerated iSCSI protocol.
٥٨		There should be no bottle neck and the provided solution should be able to achieve ratio of 1:1. This would provide low latency communication across the overall solution stack.
٥٩		Vendor should clearly detail the oversubscription ratio in the proposed solution (server downlink bandwidth to network uplink bandwidth).
٦٠		Interconnects or switching modules should be of non-blocking architecture and should provide line rate throughput with low latency of 1 microsecond.
٦١		All the Ethernet ports on the switching modules should be fully licenses and there should be no extra costs associated to it (apart from SFP modules).
٦٢		Vendor should clearly state if additional licenses are required for the future network (Ethernet), it should be clearly mentioned that how many ports are licensed from the day one of the proposed solution.
٦٣		The network modules (across the enclosures) should be able to communicate the data across each other without having the need of top-of-the-rack switches. This would provide low latency fabric which would enhance and speeds up the east-west traffic within the data center.
٦٤		The proposed networking components within the solution should provide SAN based FC connectivity option (along with the Ethernet); in case if the solution requires to have external storage in the future.
٦٥		The network interface card (on the compute node) should be configurable as part of the stateless computing profiles; should not be tied to a particular OS and should be managed through the unified management software.
٦٦		The downlink ports (server ports) should support Ethernet, Fiber Channel over Ethernet/CEE or Accelerated iSCSI protocol.
٦٧		The solution should be comprised of composable network resources and should provide 100/40GbE (native) & 10GbE IP connectivity between the platform and external network.
٦٨		The solution should support network switches with 100/40Gb QSP+ uplink ports, up-linkable to the data center switch.
٦٩		The enclosure should support Fiber Channel SAN switches with 32Gb FC uplinks and also at least 32Gb downlinks to all server bays. Switch should support trunking to external SAN switches at 128Gb/s per trunk.

#	Category	Item
١	SAN Storage Requirement	Offered storage shall be an enterprise storage array & 100% data availability guaranteed architecture and All Flash array only. Shall be marketed / Publish as All Flash enterprise array on the vendor web site.
٢		100% data availability guaranty shall be clearly mentioned on vendor web site for the offered model. If vendors are not supporting the 100% data availability as per their web site then vendor shall quote additional Controller and 10% additional capacity as cold spare along with array for mitigating the failure situations.
٣		The storage array should support industry-leading Operating System platforms & clustering including: Windows Server 2016, VMware 6 & 7, Solaris and HP-UX etc.
٤		Offered Storage shall be supplied with at-least Dual controller and shall be scalable to at-least Quad controllers. Vendor shall ensure that all controllers, with and without scalability, shall be connected to a common back-plane and shall not use any loosely connected architecture like through SAN Switches, Ethernet Switches, InfiniBand switches etc.
٥		Offered Storage array shall support combination of SAS SSD as well NVMe SSD inside the storage array and shall be scalable to at-least 1500TB of native raw capacity while using the combination of drives.
٦		Offered storage shall support more than 550 Flash drives.
٧		Offered Storage shall be able to protect at-least 2 drives failure simultaneously within a given raid group.
٨		Vendor shall offer only the encrypted drives with appropriate encryption licenses and shall meet FIPS 140-2 – Level 2 security requirements. Vendor shall not offer any controller based or Software based encryption.
٩		Offered FIPS 140-2 Validated encryption drives shall support both KMIP 1.3 and KMIP 1.4 for key management solutions. Vendor shall offer at-least internal Key manager engine for key management.
١٠		Controllers shall be true symmetric active-active so that a single logical unit can be shared across all offered controllers in symmetrical fashion, while supporting all the major functionalities like Thin Provisioning etc.
١١		Each and every volume created on the storage array shall be accessible by all controllers simultaneously.
١٢		Offered Storage array shall be configured in a No Single Point of configuration including Array Controller cards, Cache memory, FAN, Power supply etc.
١٣		Offered Storage array should have at-least 2TB protected DRAM cache and shall be scalable to at-least 4TB without replacing the existing controllers. Cache shall be global and coherent.
١٤		Cache shall be completely dynamic for read and write operations and vendor shall not offer any additional card / module / drive for write cache operations.
١٥		Offered storage shall be based upon latest generation Intel CPUs, Minimum Skylake series, and shall be supplied with at-least 80 numbers of CPU cores, Scalable to 160 CPU cores without replacing the existing controllers.
١٦		Offered Storage array shall have minimum of 16 x 32Gbps Fiber Channel ports 8 x 25Gbps ISCSI ports. All ports shall have capability to work at line speed.
١٧		Offered Storage array shall be scalable to at-least 32 x 32Gbps Fiber channel ports and 16 x 25Gbps ISCSI ports.
١٨		Offered Storage array shall have minimum of 32 SAS lanes in the back-end for disk connectivity running at 12Gbps speed and shall be scalable to 64 SAS Lanes without replacing the existing controllers.
١٩		Offered Storage array system shall be supplied with two additional native 10Gbps IP ports for storage based replication and shall be scalable to 4 Native 10Gbps IP ports. All ports shall be provided with SFP+ transceiver for fiber connectivity.
٢٠		Offered Storage shall have dedicated, separated processing engines, apart from CPU cores, for effectively handling of NVMe parallelism (Command queue and no. of commands per queue), Raid-Rebuilding and data striping, thin re-claim etc.
٢١		Storage array shall be supplied with at-least 8 dedicated above processing engines either in the form of ASICs or other equivalent technologies and shall be scalable to at-least 16 such engines without replacing the existing controllers.
٢٢		In case vendor doesn't have above functionality using dedicated, separated processing engines then additional 32 CPU cores shall be provided for balancing the performance.
٢٣		Offered Storage array shall have native virtualization support so that volumes can be carved out from a logical space instead of dedicating separate physical disks for each application.
٢٤		Storage system shall have distributed Global spare space. Global spare space shall be configured as per industry practice.
٢٥		Offered storage array shall support inline data efficiency engine (Supporting Thin Zero detect and re-claim, De-duplication and Compression) and shall be enabled by default. Vendor shall have flexibility to enable / disable the data efficiency engine at the time of Volume creation.
٢٦		Storage subsystem shall be supplied with Thin Provisioning, Snapshot, De-duplication, Compression, Performance Monitoring, and Quality of service on day 1 for the maximum supported capacity of array.
٢٧		Offered Storage array management console shall be able to manage at-least 8 arrays from a single console. Management console shall provide following functionalities:

٢٨		Common Dashboard for all managed arrays through a single management console.
#	**Category**	**Item**
٢٩	SAN Storage Requirement	Data migration through same console for all supported heterogeneous arrays
٣٠		On-premise analytics like performance analysis, workload planning etc. through a single console.
٣١		End to end connected topology view in pictorial format within management console, from Hypervisor to Storage arrays. At-least one of the hypervisor among VMware of Hyper-V shall be qualified.
٣٢		In case, vendor need any additional service like clustering / federation for managing multiple arrays from a single console – then all required accessories like dual Ethernet switches, cables shall be provided upfront for at-least 8 arrays.
٣٣		In case of power failure, storage subsystem shall have de-staged mode so that un-committed information can be protected. De-staging shall happen to redundant vault drives and vault drives shall be encrypted.
٣٤		Vendor shall not use any Vault drive as data drives for capacity calculation. Vendor shall not consume any additional drive slot in the drive enclosure for vault drives.
٣٥		Offered storage shall have cloud enabled monitoring, AI support and analytics engine for proactive Storage management and risk mitigation. All required licenses for same shall be included in the offer.
٣٦		Cloud Enabled Monitoring and analytics engine shall have capability to provide following:
٣٧		Providing Firmware upgrade and patch upgrade recommendations proactively along with release notes and with awareness of the peripheral infrastructure connected to the array.
٣٨		Dashboard shall clearly highlight whether there is any issue with array with respect to best practices and shall recommend the required action, if any.
٣٩		Providing extremely granular per-minute historical capacity and performance trend analysis by default, without the need to enable extra logging, install any appliances (physical or virtual), or install any software.
٤٠		Providing overall saturation level of the array while combining while analyzing various parameters like IOPS, MB/sec, Block size etc.
٤١		Providing the status of at-least top 5 volumes where latency is extremely high.
٤٢		Vendor cloud enabled monitoring and analytics engine shall be completely integrated with their support team so that it can provide history of support cases logged with Support team under different column like Critical, Normal and low severity along with closed cases. Cloud monitoring tool shall be able to provide the complete month-wise breakup.
٤٣		Shall be able to provide the executive Dashboard covering various critical and must aspects of Total Capacity, overall health / wellness score of array. De-duplication and compression ratio, over-all front-end performance etc.
٤٤		Cloud enabled Analytics engine shall have capability to provide following:
٤٥		Shall have capability of global learning – Analytics engine shall collect control information from at-least 50000+ arrays across vendor installed base for meaningful output. Vendor shall provide the documentary proof for it.
٤٦		Analytics engine shall have capability of proactive recommendation for arresting the issues / problems noticed at other install base of vendor after identifying the problematic signature.
٤٧		Cloud enabled monitoring and analytics engine integration with Hypervisor
٤٨		Offered Cloud enabled monitoring and analytics engine shall be tightly integrated with Hypervisor layer and shall be certified to work with at-least VMware.
٤٩		Hypervisor integration shall be able to provide end to end monitoring of hypervisor Datacenter, Data-store, Hypervisor Host and VMs running within the hypervisor datacenter and shall be able to link with offered storage array.
٥٠		Cloud monitoring and integration tool shall provide the detailed analysis of CPU Contention, Memory contention, IO contention for each VM – including the latency.
٥١		Cloud monitoring and integration tool shall have capability to identify the top VMs which are contributing towards maximum IOs and Latency.
٥٢		In case vendor doesn't support the above offered functionality then Vendor shall supply the enterprise license for VMware vRealize suite for at-least 20 Physical servers, each running with dual physical CPUs.
٥٣		Offered Storage management engine shall have in-built on-site edge analytics for performance engine, without connectivity to Internet / Intranet and shall offer following functionalities: All required license for offering this functionality shall be offered.
٥٤		Shall have saturation panel which can depict the overall saturation level of the storage array at different time intervals instead of looking into individual parameters like IOPS, CPU utilization, Cache utilization etc.
٥٥		Shall have capability to display top 5 volumes by hotspots as well as by latency.
٥٦		If similar nature of arrays being used in the environment then offered engine shall show the top systems by saturation level within the same console.
٥٧		Shall have capability at storage for tagging the Storage volume to given host applications so that performance charts can be drawn for application instance for easy management and troubleshooting.
٥٨		Offered storage shall advise about Placement of application on best fit system based on saturation, free usable capacity and saturation forecast after application tagging.
٥٩		Offered storage shall be supplied with unlimited license for creation of application consistent copies for Oracle, SQL, Exchange, SAP HANA and VMware through Storage console GUI.
٦٠		Offered Storage shall be supplied with in-built copy management and backup S/W unlimited license for movement of data copies of Oracle, SQL, Exchange, SAP HANA and VMware to disk based backup device, public Cloud like AWS, Azure and object storage. In case, vendor doesn't support this feature then additional 100TB Front-end capacity, full featured backup s/w shall be supplied.
٦١		Offered storage array shall be tightly integrated with VMware and shall be certified for VVOL.
٦٢		Shall be certified for vVol based replication
٦٣		Shall support more than 25,000 vVol and at-least 5000VMs using Vvol.

٦٤		Shall support both compression and de-duplication.
#	**Category**	**Item**
٦٥	SAN Storage Requirement	Shall be qualified to work with both Fiber Channel and ISCSI.
٦٦		Offered Storage array shall be integrated with Red-hat OpenShift, Kubernetes and other industry K8 based container platform through CSI driver set. Vendor shall support at-least following functionalities through their CSI / CSP integration.
٦٧		Shall support both Static and Dynamic provisioning
٦٨		Shall be able to expand, re-size the persistent volumes given to statefulset applications.
٦٩		Shall be able to create and delete the snapshots.
٧٠		Shall support CSI Raw block volume as well as CSI Volume cloning.
٧١		Support for both Fiber channel as well as ISCSI.
٧٢		Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units.
٧٣		Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array.
٧٤		It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time.
٧٥		The storage array should have support for controller-based snapshots (At-least 1024 copies for a given volume).
٧٦		Offered Storage array shall support more than 32000 base volume on the storage array without snapshot and clone.
٧٧		Offered storage shall support non-disruptive online firmware upgrade for both Controllers and disk drives without any controller reboot.
٧٨		The storage array should support hardware based data replication at the array controller level across all models of the offered family.
٧٩		Offered Storage array shall support both Synchronous and Asynchronous replication across 2 storage arrays natively without using any third party or software based solution.
٨٠		Offered Storage array shall support 3 Data center solution natively where Primary site shall be able to replicate synchronously to near-by / Bunker location and at the same time shall be able to replicate to Far location asynchronously.
٨١		In case of Primary site failure – Far site shall have capability to pull the incremental information from Near-by / Bunker location natively without using any third party or software based solution.
٨٢		Offered storage array shall have capability to create the application consistency group for replication operations. Shall have flexibility to have more than 256 volumes per consistency group.
٨٣		Offered storage subsystem shall support incremental replication after resumption from Link Failure situation or during failback operations between 2DC or 3DC solution
٨٤		Offered storage array shall be true multi-tenant and shall support more than 512 Tenant per storage array. Every tenant shall be treated as a separate logical storage array with its own user control access



#	Category	Item
١	Virtualization Platform	Fully Open Source to avoid vendor lock in. However, the virtualization platform for ERP applications (eBusiness Suite), the vendor should select the best suitable and stable solution. Additionally, the vendor has to proof the stability and maturity of proposed ERP eBusiness suite virtualization platform.
٢		If the selected virtualization solution for ERP is facing challenges to implement or serious issues, MOD has the right to request changing the proposed solution
٣		Can run in a disconnected environment with no internet access
٤		Support is from one of the Top contributor to all open source projects in upstream project
٥		Should be hardware vendor independent and certified to run commodity x86 servers from vendors like Cisco, Fujitsu, Dell, HPE and Lenovo etc.
٦		Large certified plugin database for OpenStack as NetApp, Cisco
٧		Provide 3-years support for the solution
٨		Has commercial distribution for Linux Platform on which the solution is certified on
٩		Underlying Host OS Support should be included and supported for 10 years
١٠		Underlying Host OS should comply with Security Certifications like FIPS, EAL 4+ and OSPP
١١		Underlying Host OS should support Mandatory Access Control capabilities via SELinux
١٢		Should include a management portal to manage the hosts in the cluster to easily scale out the deployment
١٣		Should not include proprietary extensions and additions not available in upstream Community
١٤		Supports unlimited number of VMs on a single hypervisor
١٥		Supports more than 20 NICs per V
١٦		Supports unlimited number of HyperVisors per Cluster
١٧		Supports unlimited number of VMs per Cluster
١٨		Supported with SELinux to secure VM isolation
١٩		Supports VM Live Migration
٢٠		Certified guests Microsoft Windows Server 2012/2012R2/2016/2019, Microsoft Windows 7/8/10, Red Hat Enterprise Linux 5/6/7/8, SUSE Linux Enterprise Server 10/11/12
٢١		Supports Highly available deployment
٢٢		Supports Multiple Pluggable SDN solutions as Cisco ACI, Nuage VSP, Juniper Contrai
٢٣		Provides Bare Metal as a Service tightly connected to the Software Defined Network and Software Defined Storage fabric
٢٤		Infiniband Support
٢٥		SR-IOV support
٢٦		CPU Pinning support
٢٧		Support for NUMA Passthrough
٢٨		Support for GPU Passthrough
٢٩		Support for Jumbo Frames
٣٠		Huge Pages support
٣١		TCP/IP Offloading
٣٢		Ironic Multi-Tenant Networkin
٣٣		Ability to Evacuate, DownScale, Maintenance Mode and Removal of nodes
٣٤		Ability to ScaleOut the compute nodes to add more processing power
٣٥		Supports In Place Upgrades
٣٦		Supports tight integration with Container Platform.
١	Support and Operation Services	Vendor Support and Subscriptions are required for 3-Years at minimum, starting from Project Handover date.
٢		RMA's should be handled by the bidder.
٣		Resident Engineer/S for 3-Years
٤		The contractor should prepare operation, upgrade & escalation procedures and manuals for efficient operations. The quantity and content should be agreed with MOD.

#	Category	Item
١	Professional Services	Detailed and intensive site-survey is a must for all sites before ordering, and preferably during bidding to ensure proposing the correct BOQ and avoid missing any items.
٢		Any missing items during the implementation that affects the setup, or the end-to-end architecture will be the bidder responsibility.
٣		The bidder shall provide all designs and architecture development from the main vendor aka (HLD, LLD, NIP,NRFU) and testing.
٤		Design and Configuration should not suffer from any SOF (Single Point of Failure).
٥		Racking and Stacking along with the needed configuration in all sites are the bidder responsibility.
٦		Environmental readiness in all sites where the cabinets will be installed is the bidder responsibility, aka (Cabinets, Powering, Cooling, Cabling..etc)
٧		Installation, Configuration, and Integration must be from the main vendor.
٨		Project management and all coordination tasks are part of the bidder responsibility.
١	Training Services	The bidder shall provide all needed and specialized training classes/seats for all components and technologies provided for 5x members in each class.
٢		If the class is associated with online/international certifications, the bidder must include all the fees associated.
٣		Classes preferred to be within the kingdom but not on-site.
٤		Out-of-Kingdom classes (if needed/offered), accommodation and transportation fees should be included in the seat charges.

ملحق (٥): معايير الأمن السيبراني

#	Category	Item	Yes/No	Evidence
1	MINIMUM-SECURITY REQUIREMENTS	Develop and maintain project management documents that include at least the following (Project plans, Project charters, Resource agreements and breakdown structure and Responsibility assignment matrix).		
2		Perform risk assessments in the early stages of projects.		
3		Define and maintain a project risk register for each project.		
4		Ensure that external information system services providers: • Comply with MoD's cybersecurity requirements. • Employ appropriate cybersecurity controls.		
5		Document and approve Service-level agreements (SLAs) for external information system services.		
6		Restrict access to system media including both digital and non-digital media, digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-digital media includes paper and microfilm.		
7		Maintain accountability and guarantee the protection and control of all digital and non-digital media during transport outside of controlled areas using defined security measures (e.g., locked container, cryptography) that are MoD-approved, or compliant encryption technologies.		
9		Prohibit or restrict the use of non-approved media on MoD information systems.		
10		Enforce data classification via software controls.		
11		Ensure that backups are properly protected via physical security and encryption when they are stored and moved across the network.		
12		Encrypt all sensitive systems data during transmission.		
13		Encrypt all sensitive systems data during storage.		
14		Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		
17		Enforce sharing information decisions by authorized system and information owners.		
18		Archive the data in secure storage locations.		
19		Back up the archived data.		
20		Archive "Top Secret" and "Secret" data and shall be protected using by National Cybersecurity Authority approved encryption mechanisms.		
21		Ensure to implement data loss prevention as per "Data Protection Policy"		
22		Conduct privacy impact assessments for systems, programs, or other activities as per "Data Protection Policy"		
23		Document and approve of a matrix to manage user permissions and authorization based on the following access control principles: • Need-to-Know Principle. • Segregation of Duties Principle. • Least Privilege Principle.		
25		Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of MoD's Data Security Standard.		
26		Document and approve the discloser of and access to MoD data to external users (e.g., external partners, allies, third party, local agencies employees) and limit it based on the Need-To-Know principle.		
27		Enforce security requirements for remote connections to systems. This includes: • Strong passwords. • Two-factor authentication. • Use of encrypted Virtual Private Networks (VPNs) per MoD's VPN security Standard. • Secure management of Secure Shell (SSH) keys. • Employing valid TLS certificates obtained from a recognized Certificate Authority (CA).		
27		Ensure that all the information systems are registered and tagged upon receipt for to maintain an accurate list of assets within MoD's IT infrastructure.		
28		Maintain the information system inventory in a centralize Configuration Management Database (CMDB).		

29		Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.		
30		Create configurations and/or procedures for systems (laptops, iPhones, etc.) that are traveling to high-risk areas.		
31		Implement approved configuration-controlled changes to the information system.		
32		Ensure that testing does not interfere with system operations that support MoD's mission and business functions.		
33		Ensure that the security impact analyses include reviewing: • Security and privacy plans. • Policies and Procedures to understand control requirements. • System design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls. • The impact of changes on organizational supply chain partners with stakeholders. • Determining how potential changes to a system create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks. • Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required.		
34		Define, document, approve, and enforce physical and logical access restrictions associated with changes (e.g., upgrades, modifications) to the MoD information system.		
35		Develop and maintain logical and physical access control lists that authorize qualified individuals to make changes to MoD information system/component.		
36		Ensure systems under configuration control shall have automation in its access enforcement and auditing.		
37		Limit privileges to change system components and system-related information within a production or operational environment.		
38		Ensure that a standard set of mandatory configuration settings shall be established and documented for information technology products employed within the MoD information system.		
39		Ensure that the configuration settings shall be implemented and exceptions from the mandatory configuration settings shall be identified, documented, and approved for individual components within the information system based on explicit operational requirements.		
40		Ensure that the automation provides data aggregation and data correlation capabilities; alerting mechanisms and dashboards to support risk-based decision-making within the MoD.		
41		Ensure a list of specifically needed system services, ports, and network protocols shall be maintained and documented in the applicable security plan; all others services, ports and protocols shall be disabled.		
42		Employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services.		
43		Prevent program execution in accordance with MoD policies regarding authorized software use which include, but are not limited to the following: • Software shall be legally licensed. • Software shall be provisioned in approved configurations. • Users shall be authorized for software program use.		
44		Establish separation of duties and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to effectively facilitate quality control.		
45		Use software and associated documentation in accordance with contract agreements such as (software license agreements and non-disclosure agreements) and copyright laws.		
46		Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		
47		Make sure that software license tracking shall be accomplished by manual or automated methods, depending on MoD needs.		
48		Ensure usage of only licensed software and track its utilization and installation.		
49		Implement critical information management mechanisms to manage confidential information, keys and certifications, and prevent storing confidential information in containers.		
50		Isolate container infrastructure using logical or physical methods.		

51		Perform Static Application Security Testing (SAST) to scans the application source files, accurately identifies the root cause and supports to remediate the underlying security flaws.		
52		Ensure that the information system designed and configured to either physically or logically separate user functionality from information system management functionality.		
53		Ensure that the information system shall be configured to prevent users from performing any functions that are not explicitly authorized for their roles.		
54		Isolate security functions from non-security functions by means of an isolation boundary implemented within a system via partitions and domains.		
55		Ensure that the isolation boundary controls protect the integrity of the hardware, software, and firmware that perform system security functions.		
56		Implement layered structures to minimize interactions between security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) to enables the isolation of security functions and the management of complexity.		
57		Prevent unauthorized and unintended information transfer via shared system resources.		
58		Ensure that the host operating system temporary files creation /access by the server application shall be restricted to appropriate service processes and protected sub-directories.		
59		Ensure the protection of information system against the effects of denial of service attacks by employing appropriate security safeguards in accordance with mod's system security standard and mod's infrastructure security standard.		
60		Implement MoD cryptography mechanisms for ensuring integrity and confidentiality for communication and transmitted information.		

#	Category	Item	Yes/No	Evidence
1	CYBERSECURITY APPLICATION PROJECT REQUIREMENTS	Communication must be encrypted, data in transit (e.g., SSH, HTTPS, TLS, IPSEC).		
2		All Application and user traffic must go through Web Application Firewall (WAF).		
3		Conduct VA scanning on all application server.		
4		Penetration Testing must be conducted to test your application.		
5		Application assets must be protected with anti-virus		
6		Application server must have Minimum Security-Based Line.		
7		Specify Application Data Classification.		
8		Comply with NCA (ECC, CSCC) and CSCC if critical systems involved.		
9		Review and test application code for all application whether developed in-house or outsourced using at least the following (Compliance testing, Configurations review, Vulnerability assessment, Secure code review, Penetration testing and Static and dynamic analysis (to verify that the application does not contain malicious code such as a backdoor).		
10		Implement the Multi-tier Architecture principle, with a minimum of 3 tiers for external web applications that are acquired		
11		Implement secure coding practices for all in-house or outsourced developed applications.		
12		Implement input validation for all applications inputs in a restrictive manner, only allowing whitelisted inputs.		
14		Implementing Multi-Factor Authentication (MFA)		
15		Implementing the Principle of Least Privilege (PoLP)		
16		Validate that rights, requirements (e.g., file type), and processing for files uploaded is handled properly. Including scanning user uploads for any viruses and malware.		
17		Implement all critical security controls on trusted systems (e.g., the server).		
18		Adopt a development, security and operations (DevSecOps) methodology and process.		
19		Implement a secure Continuous Integration/Continuous Deployment (CI/CD) pipeline.		
20		Employ container security platforms from a trusted vendor.		
21		Implement cryptographic mechanisms for applications.		
22		Employ secure mechanisms for establishing and managing cryptographic keys.		
23		Maintain a list of commonly-used, expected, or compromised passwords.		
24		Transmit passwords only over cryptographically-protected channels.		
25		Store passwords using an approved salted key derivation function, preferably using a keyed hash.		
26		Allow user selection of long passwords and passphrases, including spaces and all printable characters.		
27		Enforce composition and complexity rules (e.g., minimum character length for long passwords).		
28		Separate logically/physically the test and development environment from production and other environments.		

29		Perform full backups for applications.		
30		The backups shall include at least the following: • Web applications' configuration backups. • Stored data and information of web applications.		
31		Retain application backups for critical applications.		
32		Archive applications backups in an offsite storage.		
33		Document all used database systems.		
34		Prohibit direct access and interaction with databases for all users except for database administrators.		
35		Prohibit to copy or transfer the databases of sensitive systems from the production environment to any other environment.		
36		Use reliable, approved, and licensed database systems.		
37		Develop a disaster recovery plan for database systems.		
38		Encrypt the database.		
39		Ensure all database systems employ central clock synchronization.		
40		Develop and manage a System Development Life Cycle (SDLC) process.		
41		Integrate cybersecurity requirements for all phases of the SDLC.		
42		Ensure outsourced partners adherence to secure code development practices and MoD security requirements.		

#	Category	Item	Yes/No	Evidence
1	CYBERSECURITY THIRD-PARTY AND SUPPLIER REQUIREMENTS	The cybersecurity requirements for contracts and agreements with third parties must include at least the following: • No discloser clauses and secure removal of MoD's data by third parties upon end of service. • Communication procedures in case of cybersecurity incidents. • Requirements for third parties to comply with appropriate MoD policies and procedures laws and regulations.		
2		The cybersecurity requirements for contracts and agreements with IT outsourcing and mange service third parties must also include at least the following: • Conducting a cyber security risk assessment to ensure the availability of risk mitigation controls before signing contracts and agreements or upon changes in related regulatory requirements.		
3		The supplier or service provider must comply with all MoD's applicable cyber security policies.		
4		The right to terminate the contractual obligation when the supplier or service provider violate the cyber security polices of MoD.		
5		The right to assess the security of the suppliers or service provider, which can include site visits, documentation review, or infrastructure security review, or compliance against the self-assessment reports provided by the suppliers or service provider.		
6		The terms of contracts and agreements with third parties must include requirements related to reporting and notifying MoD of any potential or confirmed cybersecurity incidents which may cause data loss or breach, business interruption, system damages, and insider threats.		
7		The contracted third parties must ensure the cybersecurity of all entities involved in their wider supply chain for their respective systems, system components, or system services and for the notification of supply chain compromises and results of assessments or audits.		
9		Defining Service Level Agreements (SLAs), mutual confidentiality agreements and any required agreements.		
10		Recording and reviewing identified risks during the lifetime of the arrangement with the third-party.		

#	Category	Item	Yes/No	Evidence
1	THIRD-PARTY EMPLOYEES	Screening/vetting for all external support services companies, support services, and managed services personnel working.		
2		Report any personnel termination or transfer for personnel that possess MoD credentials and/or badges, or have information system privileges within a defined period		
3		Ensure that all third-party party employee's devices install all needed MoD security controls in order to ensure there is no leakage of MoD data or files.		

#	Category	Item	Yes/No	Evidence
1	cyber	Identify and document the types of changes that control system settings.		

2		Remove unused or unnecessary software and disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized communication or unauthorized transmission of information		
3		Use network scanning tools, intrusion detection systems, and hardware security technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services.		
4		Prevent network components, server software, and firmware from being installed without verifying that the component has been digitally signed with an authorized certificate.		
5		Prevent installation unless sign recognized and approved certificates that include updated versions of software, update packages, service packs, device drivers.		

#	Category	Item	Yes/No	Evidence
1	SYSTEM AND SERVICES ACQUISITION SECURITY	Inclusion of cyber security controls in the system development environment		
2		Communication procedures in the event of a cybersecurity incident.		
3		Ensure that the developer of the system, system components or services provides a description of the functional characteristics of the controls to be implemented.		
4		Ensure that the developer of the system, system components, or services provides design and implementation information for controls that include: security-related external system interfaces, high-level design, low-level design, or source code.		
5		The developer of the system, system components or services must deliver the project with the security settings implemented.		
6		Ensuring that the terms of contracts and agreements with third parties and service providers include requirements related to reporting cybersecurity incidents and informing the Ministry of Defense in the event that the third party is exposed to a cybersecurity incident.		
7		The cybersecurity services operations centers managed for operation and monitoring, which use the remote access method, be located entirely within the Kingdom.		
8		That contracts and agreements include provisions for maintaining the confidentiality of information (Non-Disclosure Clauses) and secure deletion by the external party of the Ministry's data upon termination of service		
9		Reviewing and testing the changes made to the informational and technical assets of the Ministry of Defense before applying them to the production environment.		
10		The concerned parties in the Ministry of Defense must be informed of the major changes that are planned and made to the information and technical assets of the Ministry.		
11		Correcting security vulnerabilities identified as a result of testing and evaluation by the Cyber Security Department		
12		Manage system settings during design, development, implementation, operation, or final disposal		

#	Category	Item	Yes/No	Evidence
1	ASSET MANAGEMENT	Ensure that all information systems assets are recorded and flagged upon receipt to maintain an accurate and clear list of assets within the IT infrastructure		
2		Labeling all information system assets and related devices		
3		Ensure that at least the following information is recorded in the asset list: (a) Description of the asset: 1) the name. 2) IP address. 4) The operating system. 5) Total Disk. 6) Total Memory. 7) Classification of purpose (what is it used for). (b) the place: 1) The site. (c) Item details: 1) Model. 2) Serial Number (S/N). (d) element support: 1) Center/Department (Who uses this asset?). 2) Technical support (which center/supplier usually fixes these device issues?).		

#	Category	Item	Yes/No	Evidence

1	SYSTEM SECURITY	Separation of user functions (including user interface services) from system administration functions (for example, functions necessary to administer databases, network components, or servers).		
2		Ensure that the information system is designed and configured to separate (physically or logically) user functions from information system management functions.		
3		All records shall be sent to the Cyber Security Monitoring and Event Log Management (SIEM) system in order to manage the records and analyze their content and relationship to each other.		
4		Separate security functions from non-security functions by isolating port boundaries within the system by partitions and domains.		
5		Protect the confidentiality and integrity of communications and information transmitted both in internal and external networks and of all types of information system components.		
6		To ensure that all communications that transmit sensitive and confidential information and data between web clients and web servers use the latest secure transmission protocols such as: (a) Secure Sockets Layer (SSL) protocol. (b) Transport Layer Security (TLS) protocol. (c) Secure Remote Connection (SSH) protocol.		
7		Not to use unencrypted messaging techniques to transmit any kind of sensitive information and data in order to maintain its confidentiality.		
8		Terminate the internal and external network connection associated with the communications session at the end of the session or after a period of inactivity.		

#	Category	Item	Yes/No	Evidence
1	ESSENTIAL CYBERSECURITY CONTROLS	Allowing only whitelisting for critical systems' firewall access lists.		
2		Prohibiting access to critical systems from mobile devices except for a temporary period only, after assessing the risks and obtaining the necessary approvals from the cybersecurity function in the organization.		
3		Conducting compliance test for software against the defined MOD cybersecurity requirements		
4		Secure integration between software components		
5		Conducting a configuration review, secure configuration and Harding and patching before going live for software product.		
6		Privileged Access Management		
7		User authorization based on identity and access control principles Need to know need to use, Least Privilege and Segregation of Duties		
8		Logical or physical segregation and segmentation of network using firewall and defense – in – depth principles		
9		Network segregation btween production, test and development environment		
10		Intrusion Prevention System (IPS) and Security Domain Name Service (DNS)		
11		Cybersecurity requirements for protecting and handling data must implement: • Data and information ownership. • Data and information classification and labeling mechanisms Data and information privacy		
12		Cybersecurity requirements for cartography must implement: • Approved cryptographic solutions standards and its technical regulatory limitations. • Secure management of cryptographic keys during their lifecycles. Encryption of Data in-transit and at-rest as per classification and related laws and regulation		
13		Cybersecurity requirements for backup and recovery must implement: • Scope and coverage of backups to cover critical technology and information assets Ability to perform quick recovery of quick recovery of data and system		
14		Cybersecurity requirements for Vulnerabilities: • Vulnerabilities assessments. • Vulnerabilities classifications based on criticality level. • Vulnerabilities remediation based on classification and associated risk level.		
15		Cybersecurity requirements for Penetration Testing: cope of penetration tests which must cover Internet-facing services and its technical components including infrastructure, websites, web applications, mobile apps, email and remote access.		

16		Non-disclosure clauses and secure removal of organization's data by third parties upon end of service.		
17		Requirements for third-parties to comply with related organizational policies and procedures, laws and regulations.		

#	Category	Item	Yes/No	Evidence
1	CRITICAL SYSTEMS CYBERSECURITY CONTROLS	Prohibiting remote access from outside the Kingdom of Saudi Arabia		
2		Using multi-factor authentication for privileged users, and on systems utilized for managing critical systems stated in control.		
3		implementing a high-standard and secure password policy.		
4		Utilizing secure methods and algorithms for storing and processing passwords, such as: hashing functions.		
5		Prohibiting direct access and interaction with databases for all users except for database administrators. Users' access and interaction with databases must be through applications only, with consideration given to applying security solutions that limit or prohibit visibility of classified data to database administrators.		
6		Applying security patches and updates at least		
7		Encrypting the network traffic of non-console administrative access for all technical components of critical systems using secure encryption algorithms and protocols.		
8		Reviewing and changing default configurations, and ensuring the removal of hard-coded, backdoor and/or default passwords, where applicable.		
9		Protecting systems' logs and critical files from unauthorized access, tampering, illegitimate modification and/or deletion.		
10		Logically and/or physically segregating and isolating critical systems' networks.		
11		Reviewing firewall rules and access		
12		Prohibiting direct connection between local network devices and critical systems, unless those devices are scanned to ensure they have security controls that meet the acceptable security levels for critical systems.		
13		Prohibiting critical systems from connecting to a wireless network.		
14		Protecting against Advanced Persistent Threats (APT) at the network layer		
15		Prohibiting connection to the internet for critical systems that provide internal services to the organization.		
16		Protecting against Distributed Denial of Service (DDoS) attacks to limit risks arising from these attacks.		

#	Category	Item	Yes/No	Evidence
1	DATA CYBERSECURITY CONTROLS	Screening and Vetting Candidate in job related to data migration who have access to the data.		
2		Strict restriction to allow only minimum number of personnel accessing, viewing data based on list of privileges limited to Saudi national employees.		
3		Disabling the print screen or screen capture on the devices		
4		Using of BYOD devices is prohibited		
5		Using watermark feature to label the whole documents		
6		Using Data Leakage Prevention -DLP- technologies and Right Management technologies.		
7		Implement controls to protect data: (Data Masking and Data Scrambling		
8		Using secure and up-to-date cryptographic methods and algorithmic when transmitting data for overall network communication medium as per the requirements of "advances level" in the National cryptographic stander (NCS-1:2020)		
9		Requiring contractual commitment to securely dispose MOD ministry data at the end of the contract or case of contract termination, including providing evidences of disposal the MOD		
10		Documenting all data sharing operations within Third party, including data sharing Justification.		
11		Requiring third party to notify the MOD in case of cybersecurity incident that may affect data that has been shared.		
12		Screening or vetting consultancy services employees who have access to the data		

13		Requiring contractual commitment by consultancy service including employees Non-Disclosure Agreement and secure disposal the MOD data at the end of the contract or in case termination, including providing evidences of such disposal to MOD		
14		Before sharing data with consultancy services using Data Masking, Data Scrambling.		

#	Category	Item	Yes/No	Evidence
1	FIREWALL CONTROLS	Comply with Firewall Security Standard		
2		Control the flow of network traffic between networks or hosts that employ differing security postures to increase the protection for internal networks and hosts		
3		Follow the “least privilege" principle and deny all inbound and outbound traffic by default on all Firewall implementation		
4		Use Firewall filters to restrict or block system services based on MoD ports, protocols, services Management database and best practices		
5		Treat the firewall configurations and associated documentation as confidentially sensitive information and it must be available to only authorized personnel (e.g. authorized administrators, auditors, security oversight personnel)		
6		The firewall must have at least three (3) interfaces, one for the internal network area, the second for the untrusted external network area, and the third for an intermediate security area		
7		Configure Firewall to detect and prevent all type of denial-of-service attacks including flooding attacks, ICMP flood, SYN flood, IP address sweep attack, IP Spoofing, TCP/UDP sweep attacks and port scanning attacks		
8		Define physical and logical access control for firewalls based on Access Control Standard		
9		Deploy firewall on a dedicated machine with all the unnecessary and/or non-secure functions, ports, services and protocols being disabled		
10		Firewalls shall include at least one or more intrusion detection and/or intrusion prevention methods\systems.		
11		Submit a diagram and/or a list of permissible paths and a description of permissible services accompanied by a justification for each firewall for approval prior to the deployment of a firewall		
12		All firewall interfaces shall be assigned a security zone in accordance with the network it protects. All inter-zone and intra-zone connections should be denied by default.		
13		Restrict firewall administration access to be allowed only by connecting through a console cable to a dedicated terminal or alternatively through privileged identity management system (where applicable).		
14		Install firewalls only on a hardened and routinely patched operating system.		
15		Use firewall in conjunction with a router when connecting to the Internet to prevent denial-of-service attacks and successful cracker penetrations.		
16		Firewall activities must be logged and monitored on a continuous basis		
17		Store firewall logs in a secure central logging server with NTP synchronization enabled.		
18		Back up Firewall logs on a regular basis. Store and maintain Logs for future reference and/or legal protection requirements		
19		Install firewall patches and the patches must be tested		
20		Back-up Firewall configuration settings periodically and before applying updates to ensure that existing settings are not inadvertently lost		

#	Category	Item	Yes/No	Evidence
1	IDPS CONTROLS	Use multiple types of IDPS technologies such as (network-based, wireless, network behavior analysis (NBA and Host-Based)) to achieve more comprehensive and accurate detection and prevention of malicious activity.		
2		Ensure the selected IDPS products are sufficiently reliable to meet MoD security requirements.		
3		Continuously update the IDPS databases with the latest attack signature information changes.		
4		Ensure that the IDPS send information to centralized logging servers and Security Information and Event Management (SIEM) solutions to perform log analysis and send alerts.		
5		Monitor and scan inbound communication traffic of IDPS systems 24 hours, 7 days a week for unusual and unauthorized activities.		